WISP 2019 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

12-15-2019

What do you fear?: A study on user generated health data and privacy behavior

Krutheeka Baskaran

Saji K. Mathew

What Do You Fear?: A Study on User Generated Health Data and Privacy Behavior

Krutheeka Baskaran[1]
Indian Institute of Technology Madras,
Chennai, Tamil Nadu, India

Saji K Mathew
Indian Institute of Technology Madras,
Chennai, Tamil Nadu, India

ABSTRACT

Health tracking wearables used outside the clinical settings to monitor an individual's health are widely used recently despite the information privacy concerns these devices evoke. Academic research addressing the effect of fear appeals on information privacy in the context of user-generated health data is scarce. It is important to understand what is an individual's perspective on health data privacy and the influence of fear appeals on privacy behavior. The present exploratory qualitative study captures an individual's perspective of information privacy on health data from 27 respondents using an adapted extended parallel process model. The study reveals what individuals perceive as threats and their extent of efficacy to handle the concerns over information privacy. It is observed, fear appeals influenced the respondents to choose between danger control or fear control behavior. This study provides an insight into the importance of an individual's privacy and their behavioral change, which could prove useful for manufacturers and regulators.

Keywords: privacy, digital healthcare, wearable, user generated health data, fear appeals, Extended Parallel Process Model.

[1] Corresponding author. ms17s003@smail.iitm.ac.in

INTRODUCTION

Over the last few years, especially since the introduction of the Fitbit fitness tracker in 2009, digital healthcare has taken a new turn. According to McKinsey, which published a report on the Internet of Things, around 130 million customers use fitness trackers and by 2025 it is estimated to rise to 1.3 billion (Manyika et al. 2015). Despite numerous benefits associated with these devices, there is a large quantum of real-time health data that is being stored by the vendors who provide the wearable products along with the accompanying services using the user-generated health data. Such a large quantity of health data along with analytical tools can give rise to predictive models in domains like marketing, patient care and drug development (Raghupathi and Raghupathi 2014). This wealth of health data could be collected and amassed into vast collections of data sets which would also prove to be quite useful to pharmaceuticals and insurance companies (Erdmier et al. 2016). On the other hand, such health information processing for secondary purposes could be considered private and sensitive and can pose data privacy threats. In recent years there have been several reports of health data being stolen and citizens being affected due to security breaches (Equifax 2018). According to reports, cybercrime has risen over 27% over the past years and is costing organizations on an average of US$17 million (Accenture 2017). Healthcare organizations reported the highest average cost of data breaches of over $380 per stolen record (IBM Security 2017). The user community of wearables, seem to be concerned about the processing of highly sensitive data online and several studies have reported this to be an issue in the adoption of digital healthcare (Li et al. 2016; Segura Anaya et al. 2018). Hence, we ask this question: *how do users of health tracking wearables respond to perceived data privacy threats?*

There were and are several Acts and laws being passed to protect health data like the Health Insurance Portability and Accountability Act (HIPPA), the common Rule, Privacy Act 1988(Australia), GDPR and many others across the world; although these do not clearly cover the new form of user-generated health data from devices like wearables and the companies that process these data. In many of the terms and conditions presented by the companies it is seen, there are clauses to permit selling health data to third parties (Shklovski et al. 2014). There have been several studies on the behavioral aspects of information sharing among technology users, explaining why people behave the way they do so. Further, other studies also focus on the ways to motivate users to improve the protection of their individual and organizational information (Boss et al. 2015). According to our knowledge, there is sparse research to study attitudinal and behavioral changes in individuals in response to fear appeals on their health data privacy. With a high demand for health information data, as well as recent data breaches, there is a need to explore the behavioral aspects of consumers on the use of wearables. Hence the present work focuses on understanding where the individuals stand in terms of privacy and what kind of coping mechanisms are adopted in response to fear appeals. To accomplish this objective, we have applied the Extended Parallel Process Model (EPPM) to study what threatens the privacy of an individual and what influences them to adopt different protection motivation strategies. This paper sheds light on how device usage might get affected if there is a threat to an individual's health data which could prove to be an useful insight to manufacturers.

The structure of the paper is as follows: Theoretical background gives details on the existing literature and the foundations of theory used. The methodology used to conduct an exploratory study is discussed in the next section. Followed by data analysis and presenting the thoughts from users and finally, the last section addresses the conclusions drawn and the future research path is provided.

THEORETICAL BACKGROUND

Information privacy is the concept of controlling how one‘s personal information is acquired and used (Warren and Brandeis 1890). Over the years there is very rich literature on information privacy that is dispersed across all disciplines (Smith et al. 2011). Information privacy has been studied at multiple layers of analysis and several theoretical contributions have been made (Bélanger and Crossler 2011). Privacy research has made use of several theories including, Rational Choice Theory, Theory of Planned Behavior, Privacy Calculus theory, Social Cognitive theory and Protection Motivation Theory among several others. Most of these theories explain the behavioral aspects of an individual towards privacy and their behavioral intention. We initially turned to Protection motivation theory (PMT) (Rogers 1975, 1983) to study the influence of fear appeals on behavioral intentions specifically the coping mechanism that is adopted by individuals when there is a privacy threat on their health data. Literature highlights PMT has two issues 1) predictions are inconsistent with empirical data 2) it does not explain why or how an interaction between threat appraisal and coping appraisal occurs or how it leads to protection behaviors (Witte 1992). Studies related to health data privacy such as in this work require us to understand how people cognitively deal with danger or threats by denying or defensively avoiding the threat while choosing to use/not use the wearable device. From literature, it is observed that theories using coping mechanisms, such as EPPM, are found to be versatile in capturing human behavior (Liang et al. 2019). Hence, this motivated us to choose the EPPM for this study.

The EPPM is based on elements of Hovland, Janis and Kelly's fear–as-acquired drive model (Hovland et al. 1953), Leventhal's danger control/fear control framework (Leventhal 1970), Roger's original PMT (Rogers 1975) and further goes on to explain the fear control process in detail. Fear appeals is a persuasive message that intents to play on individual's fear and motivate them to take a certain action. In the model adapted from EPPM Figure 1, the elements of fear appeal are severity of the threat, the individual's susceptibility to the threat and feel of efficacy to perform recommended responses.

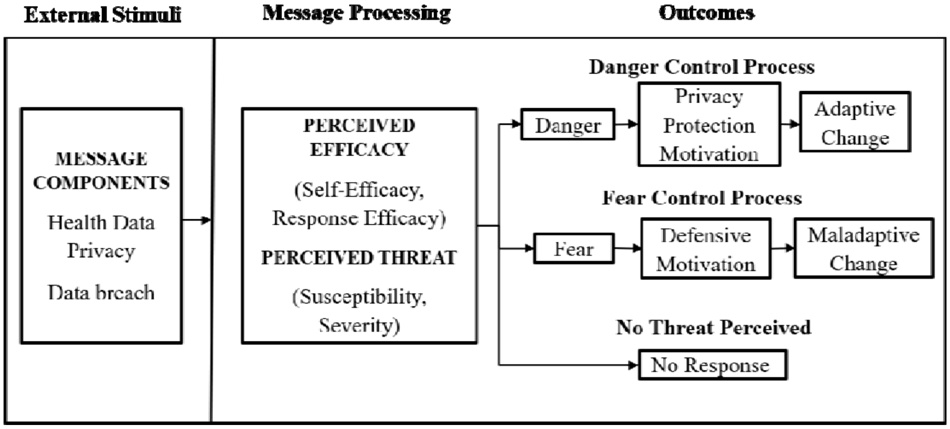
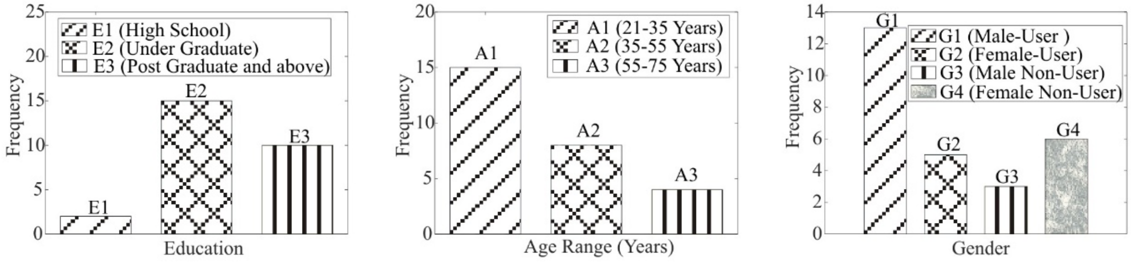


Figure 1. Adapted Extended Parallel Process Model

Threat is defined as danger or harm that exists in the environment irrespective of our knowledge. Individuals' perception of threat or Perceived Threat has two parts: perceived susceptibility and perceived severity, where the former refers to beliefs of one's vulnerability to the threat and the latter refers to the individual's belief about the magnitude of the threat. Whereas, Self-efficacy is an individual's belief of the ability to perform the recommended response and Response Efficacy is the effectiveness of the recommended response to be able to avert the threat (Witte 1992). The EPPM also posits that upon exposure to fear appeals the individual reacts in three ways 1) no-response 2) danger control responses 3) fear control responses. The difference between the original EPPM model and our adapted model is that we have brought out two dimensions: danger that will influence a rational or protection motivation behavior and fear that will induce a defensive motivation. This model has potential to capture an individual's reactions to fear appeals on privacy of their health data and their behavioral and attitudinal outcomes towards these threats. In recent times, there were highlights in the literature that showed that EPPM still has a potential for a theoretical model at present in IS (Information Systems) research (Johnston and Warkentin 2010; Roberto 2013; Liang et al. 2019), which all the more gave us another reason to choose this theory as a foundation for our study.

METHODOLOGY

An exploratory research design has been followed; in this study we have made use of a qualitative research methodology due to the subjective nature of an individual's behavior given a situation. In order to get a complete understanding, we have used a purposive sampling method, wherein interviews were conducted with users (18 respondents) as well as non-users (9 respondents) of wearable fitness trackers. Figure 2 summarizes our interviewees demographics. The age, educational background and gender variations were taken into consideration to cover a vast range of people; the subjects' age ranged from 21-65 years. The age of half the respondents is between 21 and 35 as they represent the larger population who are either using the device or are potential users. Semi-structured questions were developed in comparison to the risk behavior diagnostic scale developed for the EPPM (Witte 1996). The questions where initially piloted with a few respondents and their comments were taken into consideration to produce an understandable set of interview questions. Personal in-depth interview, with a semi structured interview guideline, was conducted with all the subjects. Each interview lasted between 20-30 minutes, were audio recorded with consent and then manually transcribed. The questions in the interview were structured to cover all aspects of one’s opinion on wearable devices, their perception of privacy of their health data and a threat scenario to their privacy was introduced to gauge their behavioral outcome. Wherever required, probing follow-up questions were asked to obtain rich additional insights into the perceptions of an individual. The interviewees were informed that their participation in this interview was voluntary and strict confidentiality of their identity will be maintained. The interview recordings were transcribed, and the authors analyzed the content of the transcript for emerging themes. Further, to strengthen the support to the themes identified manually, the content was also analyzed with the help of NVivo 12 software. Themes were coded and categorized under each EPPM construct.



(a) (b) (c)

Figure 2. Respondents Demographics based on Education (a), Age range (b) and Gender (c)

RESULTS

Analysis of the interviews revealed several interesting results about the behavioral outcomes of individuals facing privacy threats. Health data privacy and data breach form an important part of the questionnaire and the responses from the stake holders are classified based on the constructs that has been proposed in the model.

Perceived Threat

One can only protect oneself if one knows there is a threat; the first general question to everyone was ‘How private do you think your wearable health data is?’ Most of the respondents feel that their health data is quite private to them and they would not want anyone to have access to it unless they consent to it. For example, one of the respondents said "*Though I do try a lot, I progress very little in trying to reduce my weight. So, this data is sensitive to me. Sometimes I don't even like telling my husband what I weigh.* There were a few others who felt the health data that their wearable device stores is not that sensitive and if they know who is using it or who has access to it, they are fine with sharing their data. One respondent is quoted as *"It is only a few height and weight parameters. I don't mind sharing it as long as I know what it is used for and who is using it".*

From the general classification of perceived threat, the construct is subdivided as perceived threat due to susceptibility and severity. Of the themes categorized under threat susceptibility, we found weak security measures by the company and too much information sharing online were highly quoted. One the respondents felt: "*Some of these devices had GPS tracking that showed the exact location I was at while exercising, a very easy target for stalkers you can say. Even after turning off the settings I kept having a feeling I was watched. I feel the threat is real."* Many of the respondents also felt the security measures by the service providers would be a major factor: "*Unauthorized access to my data would be only by hackers. But that is also due to the negligence or weak security measures of the company. If they kept all the data security up to date and they were vigilant I don't think this can take place."*

Perceived severity is the perceived degree of harm associated with a privacy breach of an individual's health data. People are less likely to take no action when the severity of threat is high (Rogers 1983). The respondents most often highlighted that the loss of privacy negatively impacts peace of mind: "*I would try and trace out how it got leaked and whose fault was it. If it was a big corporate like the device company, you say maybe I might stop using it and might tell others too to not use it too. But that is all I can do I think right what else you can do. But I will* *lose my peace of mind I am sure of that".* The second most mentioned perception was the notion that loss of personal data led to exposing themselves to another person: "*The main thing is location, since I am always wearing it; it also knows my complete day plan so that is a threat (sic). There is also an app called Strava which I used to use when I run or swim. I stopped using now as I realized that anyone can see me on the map where I have walked or which path I have taken, it is all public. It's like someone can always track me".* Concerns were raised by several respondents that the loss of their data like location, can also lead to physical security issues with stalkers. Many also felt the notion of their data being seen by someone made them feel embarrassed as they were not in good physical shape and they do not want anyone watching or storing that image of them.

Perceived Efficacy

Perceived efficacy refers to an individual's ability to carry out recommended responses to avert threat and the individual's belief of if the response effectively would prevent threat; the former is called self-efficacy and latter is called response efficacy (Rogers 1983; Witte 1992). It is seen that only if an individual is exposed to a threat that they perceive as harmful, will there be an appraisal of efficacy (Johnston and Warkentin 2010). Majority of the respondents in our study mentioned the themes: interest in using technology or tech savvy and awareness about privacy as strong influencer of self-efficacy: "*As a person exposed to gadgets a lot, I understand the workings of data as a business commodity. But on the other hand, people like my parents who use this do not know the implications of a privacy breach unless explicitly educated".* The second close contender was previous exposure to technology or wearable devices and individual's personality traits. In addition, when interviewees were asked about how they knew if a particular response will help them, they overwhelmingly stated that they had no idea about proper privacy preserving etiquettes online unless the information is passed to them from the company or their peers and close ones: *"If there is breach what I would do? I don't know, maybe wait for the company to resolve it. But once the data is lost it is lost forever right."*

It is seen, from an individual's degree of belief that one can perform a response to minimize the effect of the threat, the individual might choose one from three paths: danger control response, fear control response or no response according to the proposed model. If an individual feels that he or she does not have the efficacy to reduce the threat then the individual would resort to fear control responses like denial and, defensive avoidance: *"I am not bothered about privacy issues now. My focus is on the fitness service of the gadget. Moreover, who would want data like my height and weight"*. If an individual has a strong belief on one's self ability to avert threat then the individual would resort to attitude or behavior change, referred to as danger control responses (Witte 1992).

Finally, coding with the help of the NVivo software helped us gain insights into interesting perceptions based on demographic details as shown in Figure 3. Males had a higher perception of efficacy while females on the other hand had higher threat perceptions, meaning men were more confident in their ability to avert the threat while women felt the threat value was higher than their ability to avert. Comparison of perceptions of different age groups within a gender also

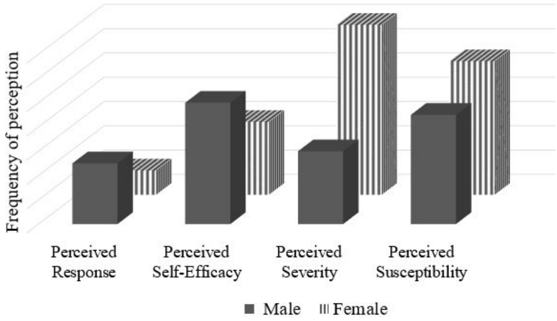
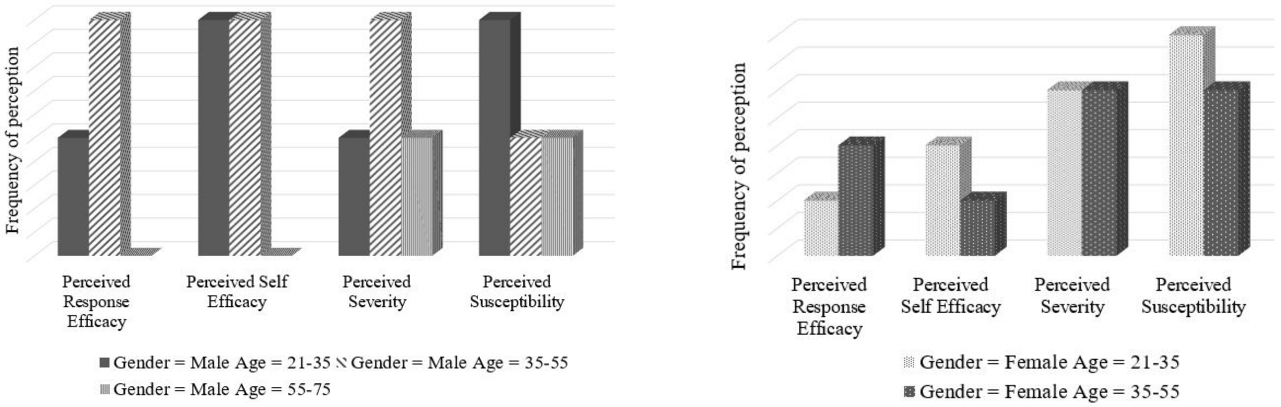


Figure 3. Gender comparison of perceptions

shows that men between the ages of 21-35 feel self capable of averting threat; men between the ages of 35-55 feel that there would be severe consequences to a data breach i.e. higher perceived severity and men between the ages 55-75 have very low perception of efficacy (Fig. 4a). On the other hand women of all ages feel more vulnerable and fear the severity of consequences of a data breach and younger women have slightly higher perception of efficacy than older (Fig. 4b).



(a) (b)

Figure 4. Age Comparison of perceptions within gender

DISCUSSIONS

This study adapted the EPPM model originally used for health protection behaviors to understand if it would also elicit a similar response for privacy protection behaviors. This paper tries to understand the contradictory behavior of individuals towards privacy through the lens of fear appeals. Based on the EPPM model we have evaluated the outcomes of the responses and mapped them to fear control and danger control cognitive perceptions.

As shown in equation below we found, when the perceived threat is high, and efficacy is low respondents chose an emotional process or fear control process wherein they address their fears rather than the danger at hand. The themes elicited showed “denial”, “blame games”,” ignore the threat” as ways of respondent dealing with their fears. Some of the respondents still chose to keep using the device and sharing their health data as they felt the benefits of the device outweigh the threat of privacy loss. The rest of the respondents chose to ignore it or exhibited wishful thinking saying nothing bad can happen. On the other hand, when the perceived threat as well as the efficacy is high, respondents realize they are in risk for a severe danger and become motivated to protect themselves. This was highlighted in the themes coded from the interviews which stated, “stop using a wearable”, “restrict sharing information” “make sure the privacy settings are in place” as some of the protection measures taken. The respondents, mostly educated male users of all age groups, resorted to exhibiting a protective behavior by thinking of what steps to be taken and whom to contact for damage control. Based on the analysis, behavioral response (y), the choice between cognitive or emotional outcome, when a respondent experiences health data breach can be expressed as follows:

$$y = f(PT, PE) \qquad (1)$$

where,

$$f(PT, PE) = \begin{cases} 0 & PT < PE \\ 1 & PT > PE \\ 2 & PT = PE \end{cases} \qquad (2)$$

where PT is perceived threat and PE is perceived efficacy. The values 0,1 and 2 represent No Response, Fear Control Response and Danger Control Response respectively.

When the respondents did not take the fear appeals message as a threat there was no response or behavioral change when the threat was introduced. The study also found that respondents who initially did not have any qualms about sharing their information had a change in their attitude when a threat was introduced. The threat message also seemed to give a sense of privacy awareness to many of the respondents who were not aware of issues rising due to privacy breach.

The respondents were presented with a scenario where their data was either sold without their consent to third parties or it was stolen. It was seen from the responses of the interviewees that those who were tech savvy and wanted to stay connected with technology had a lot more self-efficacy and thus were able to follow a danger control response than the others who did not have familiarity with technology.

Respondents who chose the fear control (13 respondents) are likely to keep using the device and ignore any threat to their data privacy whereas those that chose the danger control process(14 respondents) are more likely to stop using or not buy the devices in the first place. The numbers show that with more awareness or higher level of threat and higher efficacy; there is a possibility of people switching from fear control to danger control which could give an interesting scope for research on the future trend of privacy concerns and behaviors.

CONCLUSION

This study seeks to contribute to information privacy research, by adapting the Extended Parallel Process Model, in the context of user-generated data privacy. In doing so several themes were identified under the constructs of perceived threats and perceived efficacy which in turn led to danger and fear control outcomes. Despite the contributions, there are a few limitations in the study that may point to interesting future research opportunities. This study followed a qualitative approach with a purposive sampling technique, sample limited to a metro city in India. Further studies could benefit from a larger sample to concretely establish the results. The study is in its initial exploratory stage and as future directions, a quantitative study to validate the strength of each theme identified and to evaluate whether EPPM could be extended further to accommodate privacy studies is being carried out.

This study exhibits several theoretical and practical implications. To our knowledge, this paper is the first to study the behavior of individuals in response to information privacy fear appeals; specifically, to user generated health data (outside of clinical settings) from wearable devices.

As future directions, further studies could focus on the privacy fear appeals in different cultural settings considering technology adoption stages. Wider cultural samples in different geographic locations can give rise to a comparative study and results can be more generalizable which could prove useful to device manufacturers and policy makers. According to our knowledge there is no prior instrument to validate privacy in terms of fear appeals. Hence there is also a scope for scale development and validation in these terms.

REFERENCES

Bélanger, and Crossler. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), p. 1017. (https://doi.org/10.2307/41409971).

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837–864. (https://doi.org/10.25300/MISQ/2015/39.4.5).

Equifax. 2018. "Equifax Releases Updated Information on 2017 Cybersecurity Incident," p. 1. (https://www.equifaxsecurity2017.com/2018/03/01/equifax-releases-updated-information-2017-cybersecurity-incident/).

Erdmier, C., Hatcher, J., and Lee, M. 2016. "Wearable Device Implications in the Healthcare Industry," *Journal of Medical Engineering and Technology* (40:4), pp. 141–148. (https://doi.org/10.3109/03091902.2016.1153738).

Fife, E., and Orjuela, J. 2012. "The Privacy Calculus: Mobile Apps and User Perceptions of Privacy and Security," *International Journal of Engineering Business Management* (4:1), pp. 1–10. (https://doi.org/10.5772/51645).

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention, and Behaviour : An Introduction to Theory and Research*, (Illustrate.), Addison-Wesley Pub. Co.

Gao, Y., Li, H., and Luo, Y. 2015. "An Empirical Study of Wearable Technology Acceptance in Healthcare," *Industrial Management and Data Systems* (115:9), pp. 1704–1723. (https://doi.org/10.1108/IMDS-03-2015-0087).

Hovland, C. I., Janis, I. L., and Kelley, H. H. 1953. *Communication and Persuasion: Psychological Studies of Opinion Change*, New Haven, CT, US: Yale University Press.

IBM Security. 2017. "2017 Cost of Data Breach Study," *Ibm Security Reports* (June), pp. 1–34. (https://www.ibm.com/downloads/cas/ZYKLN2E3).

Johnston, and Warkentin. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), p. 549. (https://doi.org/10.2307/25750691).

Leventhal, H. 1970. "Findings and Theory in the Study of Fear Communications," in *Advances in Experimental Social Psychology* (Vol. 5), pp. 119–186. (https://doi.org/10.1016/S0065-2601(08)60091-X).

Liang, H., Xue, Y., Pinsonneault, A., and Wu, Y. "Andy." 2019. "What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping

Perspective," *MIS Quarterly* (43:2), pp. 373–394. (https://doi.org/10.25300/MISQ/2019/14360).

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., and Aharon, D. 2015. "THE INTERNET OF THINGS : MAPPING THE VALUE BEYOND THE HYPE," *Executive Summary*. (https://www.mckinsey.com/~/media/McKinsey/Business Functions/ McKinsey Digital/Our Insights/The Internet of Things The value of digitizing the physical world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx).

Minen, M. T., Stieglitz, E. J., Sciortino, R., and Torous, J. 2018. "Privacy Issues in Smartphone Applications: An Analysis of Headache/Migraine Applications," *Headache* (58:7), pp. 1014–1027. (https://doi.org/10.1111/head.13341).

Neff, G., and Dawn, N. 2016. *Self-Tracking*, The MIT Press Essential Knowledge Series. (http://lccn.loc.gov/2015039937).

Ponemon Institute and Accenture. 2017. *2017 Cost of Cyber Crime Study*, p. 56. (https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf).

Raghupathi, W., and Raghupathi, V. 2014. "Big Data Analytics in Healthcare: Promise and Potential," *Health Information Science and Systems* (2:1), pp. 1–10. (https://doi.org/10.1186/2047-2501-2-3).

Roberto, A. J. 2013. "Editor's Note for the Extended Parallel Process Model: Two Decades Later," *Health Communication* (28:1), pp. 1–2. (https: //doi.org/ 10.1080/ 10410236.2013. 743748).

Rogers, R. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology* (91(1)), pp. 93–114.

Rogers, R. 1983. *Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation*, (Social psy.), (R. Petty and J. Cacioppo, eds.), New York: Guilford Press.

Segura Anaya, L. H., Alsadoon, A., Costadopoulos, N., and Prasad, P. W. C. 2018. "Ethical Implications of User Perceptions of Wearable Devices," *Science and Engineering Ethics* (24:1), Springer Netherlands. (https://doi.org/10.1007/s11948-017-9872-8).

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., and Borgthorsson, H. 2014. "Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use," in *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*, Toronto: ACM, pp. 2347–2356. (https://doi.org/10.1145/2556288.2557421).

Smith, H. J., Dinev, T., and Xu, H. 2011. *Information Privacy Research : An Interdisciplinary Review*, (35:4), pp. 989–1016.

Warren, S. D., and Brandeis, L. D. 1890. "The Right to Privacy," *Harvard Law Review* (4:5), The Harvard Law Review Association, pp. 193–220.

Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communication Monographs* (59:4), pp. 329–349. (https://doi.org/10.1080/03637759209376276).

Witte, K. 1996. "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale," *Journal of Health Communication* (1:4), pp. 317–342. (https://doi.org/10.1080/108107396127988).