World Journal of Management
Vol. 7. No. 1. March 2016 Issue. Pp. 82 – 91

Wearable Device Data and Privacy: A study of Perception and Behavior

Cory Hallam* and Gianluca Zanella**

In the Age of wearable devices, managing new technologies and data generation brings to bear information security and a privacy paradox. The convergence of wearable sensor technology and personalized predictive analytics has the potential to help researchers with early detection and treatment of medical problems. However, amidst the excitement for this new healthcare scenario, the amount of personal and sensitive data flowing from wearable devices to the cloud raises concerns about data security and customer privacy. While cyber-security experts and lawmakers are already working on securing the infrastructure, privacy issues are emerging from individuals' social habits. Data from an exploratory study shows how user intent to avoid potential privacy issues disclosing sensitive personal information collides with the individual's social propensity to share wearable information, generating a potentially regrettable behavior.

Field of Research: Management Science, Managing Change, Governance

1. Introduction

Progress in science and technology creates the potential for emergent issues and dangers. As professor Stephen Hawking noted in the 2016 BBC Reith Lectures, *"We are not going to stop making progress, or reverse it, so we have to recognize the dangers and control them".* Scientists and policy makers share the burden of recognizing and managing potential issues arising from progress in science and technology (Shields, 2015). The rise of social media is a perfect example how new technology that changed social behaviors can have unexpected side effects. A major turning point for the Social Network Site industry was the establishment of Facebook in 2004. It has rapidly become the most popular social network site online, counting more than 1.5 billion monthly active users. It is so pervasive that many consider it a normal part of daily life (Lampinen *et al.*, 2011). However, the growth in Social media has also highlighted the persistent, cumulative, and searchable nature of information, with unclear boundaries between public and private data (Viégas, 2005). Privacy threats arising from blurred boundaries between online (public) and private life pushes the study of the phenomena and the establishment of new policies to protect individuals' rights (Goodwin, 1991; Solove, 2008; Clark, 2010). Literature shows that privacy is a concern for many online social media users, but individual privacy attitudes are often inconsistent with behaviors (Xu *et al.*, 2011). Many studies have found a gap to exist between the attitudes and behaviors, coined as the privacy paradox (Kokolakis, 2015).

* Dr. Cory R.A. Hallam, Center for Innovation, Technology and Entrepreneurship, University of Texas at San Antonio, TX, USA. email cory.hallam@utsa.edu, 210-458-6985.
** Gianluca Zanella, Center for Innovation, Technology and Entrepreneurship, University of Texas at San Antonio, TX, USA. email gianluca.zanella@utsa.edu, 210-458-6559.

A crucial aspect that adds complexity to the online privacy problem is the dynamic nature of the information technology industry. Because technology improves quickly, new unexpected threats to privacy are often exploited in online social networks. During the last few years, the electronics industry has improved the production of miniaturized sensors. Consequently, the prevalence of new devices designed to be worn on (and in) our bodies are multiplying fast (Piwek *et al.*, 2015). These devices seamlessly collect, store, and transmit data, some of which could be considered as private and sensitive. While HIPAA rules in the U.S. apply for the storage and transmittal of medical information (Petersen and DeMuro, 2015), many new exercise and social devices (i.e. Fitbit, etc.) produce time-series data that lends itself to the creation of what we coin "emergent medical records". These would be records of one's activity (or inactivity), that could be used by a third party to assess the individual's health and potentially impact their employment, insurance benefits, health premiums, etc. Furthermore, many of these devices use the cloud for storage and necessarily interface with social media sites for sharing such information, thus begging questions of privacy.

The most familiar devices include smart phone apps coupled with smart bands, smart watches, and smart glasses, used to monitor our health and provide quick access to online services. The data flowing from these devices to the cloud is expected to transform medicine (Bonato, 2003; Park and Jayaraman, 2003; Topol *et al.*, 2015), providing researchers with extensive and accurate data, and offering clients personal health-care analysis. However the concern is that the flow of highly sensitive data produced by wearable devices can also be easily shared online through social media networks. The complexity of this aspect of our daily lives and the gap between our knowledge and behavior has resulted in a call by many scientists, experts, and policy makers, to recognize and mitigate these threats to privacy and to educate people about it (Goodwin, 1991; Xu *et al.*, 2012; Larsen and Lawson, 2013). Among the growing literature about online privacy, no studies have successfully modeled the privacy paradox that arises due the gap between privacy concerns and online behavior (Kokolakis, 2015).

The main goal of this exploratory study is to address the gap between people's privacy concerns (perceptions) and their real behavior, and identify a potential new model for how this area of study could be expanded. Given the sensitive and personal nature of wearable device data, this research focuses on wearable devices, but the model is suggested to hold for more generic online behaviors. The first section of this paper provides a literature review about the privacy paradox and how it impacts individual behavior. We present a cognitive model that addresses the source of the gap utilizing Construal Level Theory followed by the design of the exploratory study. The final sections present the results and the implications of this exploratory study on future work.

2. Literature Review and Theoretical Underpinnings

2.1 Social Network and Privacy Paradox

The rise of online communication in the relationship development process has changed our lives, enabling individuals to connect asynchronously and synchronously with others, and expand circles of friends and acquaintances (Jones and Fox, 2009). Research in the past decade shows that social capital (Adler and Kwon, 2002) is a particularly significant outcome to consider when studying the use of social network sites (Ellison *et al.*, 2007; Steinfield *et al.*, 2008; Steinfield *et al.*, 2009; Burke *et al.*, 2010; Ellison *et al.*, 2011). The increased worldwide usage of smartphones and mobile devices has expanded the possibility for individuals to share information with other users, creating an easy and attractive means of

disseminating private, sensitive, and possibly inappropriate, harmful or even illegal information (Chretien *et al.*, 2009). Given the persistent, cumulative, and searchable architecture of the World Wide Web, private information and communications posted may be read for an extended duration by everyone and constitute the "digital footprint" of an individual. The importance of privacy concerns is highlighted by reports and studies on internet service companies (Debatin *et al.*, 2009). Concerns have been raised about the commercial use of personal information and behaviors tracked from individual's profiles (Soghoian, 2008). To address this growing problem, some countries have discussed and put into practice laws to establish an individual's right to secure or erase potentially damaging, private information. Consequently, some countries have in practice laws to prevent and punish the misuse of online information.

However the boundaries between private and public data are not always clear (Katz and Rice, 2002). What emerges in this environment is a gap between the online privacy concerns about consequences of a breach of privacy, and the behavior of disclosing online personal information (Viégas, 2005). Jones and Soltren (2005) showed that 74 percent of users are aware of privacy options on Facebook, yet only 62 percent actually used them. Users willingly post large amounts of personal information, but at the same time express concern for the risks the social network sites pose to their privacy. The gap between concerns and behavior, known as the "privacy paradox" (Brown, 2001; Norberg *et al.*, 2007), has been the focus of many studies (Kokolakis, 2015), however it is still not fully explained in these studies. Surveys indicate that people are highly concerned about their privacy and about how their information is stored and used (PEW, 2014; Patil *et al.*, 2015), but there is a low correlation between privacy attitudes and online behavior (Tufekci, 2008). The privacy paradox debate has triggered research to explain this complex phenomenon through different theories and models, and brings into play the relationship between attitudes and behaviors.

2.2 Wearable Devices and Privacy

Medical research and innovation has triggered the proliferation of small sensors that make possible wearable devices that collect and transmit data in real time (Mukhopadhyay, 2015). The first large-scale application of this type of technology was fitness tracking devices, including smart bands, smart watches, and smart phone apps. The use of wearable sensor technology supports personalized predictive analytics to detect medical problems, which in turn will enable healthcare to shift from a reactive model to a proactive model. This offers the benefit of helping healthcare providers offer better customized service to their patients while optimizing the costs. As most devices and their applications are wireless in nature, security and privacy are among major areas of concern, which may restrict people from taking advantage of the full benefits from these systems (Kotz *et al.*, 2009). The gamification (Deterding, 2012) approach used to increase the sales of these new devices pushes the social-reward side of data flowing from wearable technology, even though it may lend itself to the potential use as emergent medical healthcare data. Through a gamification lens, people are not made aware of the sensitive nature of the wearable data, exposing them to the potential long-term misuse of this information.

2.3 Privacy Attitudes and Behavior

Several important streams of research related to attitudes and behaviors apply to the privacy paradox. Privacy Calculus Theory (PCT) proposes that behavior is a resulting balance between privacy concerns and social rewards (Xu *et al.*, 2011; Jiang *et al.*, 2013). Social theory-based interpretation adopts the perspective of social networks as social collectives.

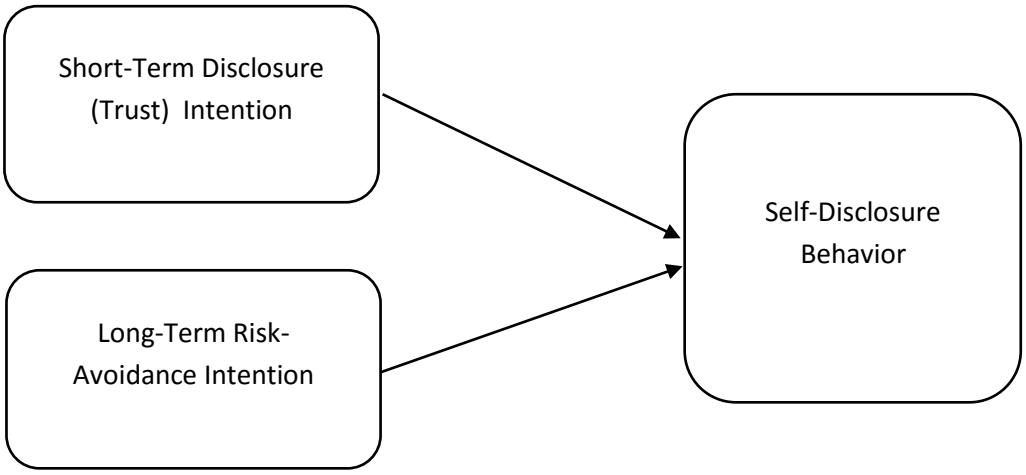
The individual perceives oneself as belonging to a community with the implicit rule to self-disclose, while the risks are associated with a more formal and abstract social collective (Lutz and Strathoff, 2014). The cognitive biases and heuristics in privacy decision-making draw from cognitive theory. This approach proposes that behavior decisions are affected by biases and heuristics, like optimism, overconfidence, affect bias, and hyperbolic discounting. In this context the individual values future benefits less than the present ones, consequently choosing self-disclosure behavior (Acquisti and Grossklags, 2005). From a bounded rationality perspective, incomplete information and information asymmetry suggests that the lack of knowledge constrains decisions. In this vein of thought, when people are provided context and knowledge, concerns are good predictors of intentions and behavior (Acquisti and Grossklags, 2005; Baek, 2014).

While these theories have all been used to attempt to explain aspects of the privacy paradox, this complex phenomenon has not been fully explained (Kokolakis, 2015). Past attempts to explain the gap suffered from a shortage of representativeness and potential biases (Baek, 2014). Reviewing these theories, we note that two are rooted in cognitive theory whereby the outcome is a balance between concerns and rewards, eventually moderated by biases and heuristics. Social theory, however, proposes the outcome as a balance between more concrete immediate social rewards and more abstract distant-future social concerns. In cognitive research literature, Construal Level Theory (CLT) (Liberman *et al.*, 2007; Trope and Liberman, 2010) shows how the choices people make every day are unconsciously based on a discounting process. In this discounting process, near and positive outcomes weigh more than distant and negative outcomes in the personal evaluation of an action, because the distance in time discounts the negative aspects of the outcome. Combining these theories, we henceforth develop a more complete model that more accurately reflects the observed behaviors associated with the privacy paradox.

2.4 The Proposed Theory

To create a better explanation of the privacy paradox, we propose a theory based on a cognitive model that combines the current theories with the CLT perspective. In doing so, we believe we can begin to explain the gap between the privacy attitudes and the behavior of the individual. Drawing from privacy calculus theory, we propose the behavior of self-disclosure as the resulting balance of two opposite intentions, namely 1) a risk-avoiding intention, which negatively affects the behavior, and 2) a trusting intention, which positively predicts the individual's self-disclosure (Figure 1). As Lutz and Strathoff (2014) observed, people are willing to provide data online because they feel their interaction with social media is like a community they are part of, whereas the calculated hazard of data misuse is perceived as hypothetical and distant. The rewards are more concrete while the risks are more abstract (Lutz and Strathoff, 2014). What is unclear is if these perceptions hold given an individual's prior exposure to negative outcomes of the associated risks.

Figure 1: Proposed Theory based on CLT



Construal Level Theory explains how any type of distance, including social, temporal or psychological, impacts our decision-making process. The positive value coming from a closer behavior is enhanced, while the negative value of a distant behavior is discounted (Liberman *et al.*, 2002; Liberman *et al.*, 2007; Trope and Liberman, 2010). Under this point of view, the gap between privacy concerns and behavior is explained taking in account the psychological distance between the self and the potential negative outcomes. Thus the more distant an individual feels they are from the breach of privacy, the less value it will have on the choice of behavior. Therefore we expect that people showing more privacy awareness will avoid privacy-critical behavior. We also expect that age and level of education will impact the disclosure behavior. The specific hypotheses for this study are proposed as follows:

- ***Hypothesis 1:*** *Short Term Self-Disclosure Intentions are positively related to disclosure behavior*
- ***Hypothesis 2****: Long-Term Self-Disclosure Intentions are negatively related to disclosure behavior*
- ***Hypothesis 3****: Age exerts a positive effect on disclosure behavior*
- ***Hypothesis 4****: Education exerts a positive effect on disclosure behavior*
- ***Hypothesis 5****: Privacy Awareness exerts a negative effect on disclosure behavior*

We contextualize our research to look at e-healthcare privacy, especially related to the use of wearable devices, as literature shows that online privacy can be segmented into different contexts (Baek, 2014), each with a different associated values (Hull, 2014).

3. Research Method and Analysis

3.1 Experiment Design

A quasi-experimental exploratory study was designed to validate the proposed theory that includes measures of intentions based on the CLT. The instrument was an online survey administered with a snow-ball technique to avoid potential biases and limitation, and improve the representativeness (Biernacki and Waldorf, 1981; Berg, 1988). The survey included a section to test the intentions and the behavior of the users of wearable devices.

3.2 Measures

All measures were based on 7-item Likert scale questions. The behavior scale has been adapted from (Jiang *et al.*, 2013). A new section has been developed for the wearable devices behavior, drawing from the Facebook behavior scale (Contena *et al.*, 2015) and from the SeBIS security scale (Egelman and Peer, 2015). Each of these tools was previously validated. We developed the instruments for the short-term and long-term intentions for wearable devices for this study. The check for internal consistency and reliability showed that they are robust enough to be used in our research (Table 1).

3.3 Results

A sample of 103 respondents was obtained using a snowball technique, with 83 completed surveys. To address potential issues about the sample size, we checked the computed post-hoc power for our results (0.98). The age of respondents was between 20 and 83, with a mean of 39.8. Forty two percent of respondents were male, and nearly 70% of the sample had a college degree. The average number of social media accounts per person was 3.5, and about 60% of the sample uses wearable devices or smart phone apps to track their daily activity. Table 1 reports the reliability coefficient alpha for the instrument (Cronbach, 1951). Moreover, we checked for multicollinearity issues (see Variance Inflation Factor, VIF, in Table 1). The instrument was found to be robust enough to test our theory. We do note that the Self-Disclosure Behavior could be reworded to achieve a better reliability, however we will track this further in future studies.

Table 1: Cronbach alpha and descriptive statistics for the latent variables

Latent Variable	Cronbach Alpha	VIF	Mean	Std. Deviation
Self-disclosure Behavior	0.65	< 2.00	2.74	0.882
Long-term risk avoid Intentions	0.80	< 1.9	5.33	1.348
Short term self-disclosure Intentions	0.73	< 1.5	2.84	1.370

We used multiple regression models with interactions to test out hypothesis. Our control variables are gender, education, privacy awareness, and age. In Model 1 we can see that the direct effects of the short-term self-disclosure intentions on the behavior are statistically significant (Table 2). As expected, short-term intentions have a positive impact on the behavior, supporting Hypothesis 1. Long-term intentions are negatively exerting an effect on the behavior, thus supporting Hypothesis 2. When adding the control variables, the main effects are still significant, with a slight change in magnitude.

The construal level effect on the behavior is evident in the results. The short-term positive effects are enhanced while the long-term negative effects are discounted. Consequently the resulting behavior is slightly affected by the privacy concerns, but is affected more by self-disclosure intentions. This finding shows that the short-term disclosure intentions have a high positive impact on the disclosing behavior. The long-term risk-avoiding intentions have a negative but smaller effect on the final behavior. Although the awareness of the threats related to an individual's privacy is high, the consequent behavior is more directly driven by the social-rewarding disclosure intention.

Table 2: Main Effects and control variable's effects (N = 83)

	Estimated Coefficients from Linear Regression Analysis				
	Model 1	Model 2	Model 3	Model 4	Model 5
Short-Term disclosure Intentions	0.308***	0.351***	0.309***	0.324***	0.300***
Long-Term risk-avoid Intentions	-0.138*	-0.148*	-0.139*	-0.118.	-0.115.
Gender			0.044		
Age		0.011.			
Education				0.089	
Privacy Awareness					-0.111*
Adjusted R2	0.204	0.228	0.195	0.211	0.236

Signif. codes: '***' 0.001 / '**' 0.01 / '*' 0.05 / '.' 0.1

In Model 2 the age as control variable shows a small and significant effect on the behavior, validating Hypothesis 3. Model 3 results show that gender does not exert any significant effect on the behavior. Surprisingly Model 4 shows that education is not significantly affecting the disclosure behavior, thus leading us to reject Hypothesis 4. Privacy Awareness exerts a significant negative effect on the disclosure behavior, because it reinforces the attention to a potential privacy breach problem thus hypothesis 5 is supported.

The overall performance of the model, even with a small sample size, has been strong enough to show how the behavior is driven more by the concrete short-term rewarding intentions than by the abstract long-term risk-avoiding intentions. In the future, our research will focus on the potential mediators of the construal level effect on the behavior, and on the antecedents of the intentions.

4. Conclusions

The convergence of social media with new wearable devices raises potential issues related to the online disclosure of sensitive data, including the creation of emergent medical records. Literature highlights a gap between privacy attitudes and social media behavior. This unexplained gap, or privacy paradox, becomes more crucial when applied to sensitive data flowing from wearable devices, whereby the user may not truly realize the impact caused by the public release of such data. In order to prevent the misuse of wearable data, it is crucial to fully explain the privacy paradox.

Construal Level Theory (CLT) shows how the value of negative outcomes generated from abstract behaviors is discounted, while the value of positive outcomes generated from concrete behaviors is enhanced. This theory has been successfully applied in many studies to address gaps of the same nature in different fields (Chapman, 1996; Arnocky *et al.*, 2013; van Beek *et al.*, 2013). Applying CLT, we show that intentions to avoid abstract privacy risk are less related to behavior than to concretely rewarding intentions to disclose personal information in social media settings. This study is the first that applies CLT to address the gap between intentions and online behavior. The snowball technique enabled us to have a representative sample, attempting to mitigate potential biases and limitations. The study does suffer from a potential social desirability bias, as is common in behavioral research that

relies on all self-reporting. However, we addressed this potential bias using an anonymous survey.

The main implication of the present research is to better explain online behavior, which is a step towards improving data privacy and management. This may also enable growth in the market for wearable devices by informing users of risks and consequences associated with wearable device usage. In the long-term, further development of this model and its antecedents may lend itself to testing simulations or other training systems that may be useful for increasing the performance of employees in the information technology and cyber security fields.

References

Acquisti, A and Grossklags, J 2005, 'Privacy and rationality in individual decision making', *IEEE Security & Privacy*, No. 1**,** pp. 26-33.

Adler, PS and Kwon, S-W 2002, 'Social capital: Prospects for a new concept', *Academy of management review,* Vol. 27, No. 1**,** pp. 17-40.

Arnocky, S, Milfont, TL and Nicol, JR 2013, 'Time perspective and sustainable behavior: Evidence for the distinction between consideration of immediate and future consequences', *Environment and Behavior***,** pp. 0013916512474987.

Baek, YM 2014, 'Solving the privacy paradox: A counter-argument experimental approach', *Computers in Human Behavior,* Vol. 38**,** pp. 33-42.

Berg, S 1988, 'Snowball sampling—I', *Encyclopedia of statistical sciences*.

Biernacki, P and Waldorf, D 1981, 'Snowball sampling: Problems and techniques of chain referral sampling', *Sociological methods & research,* Vol. 10, No. 2**,** pp. 141-163.

Bonato, P 2003, 'Wearable sensors/systems and their impact on biomedical engineering', *IEEE Engineering in Medicine and Biology Magazine,* Vol. 22, No. 3**,** pp. 18-20.

Brown, B 2001, 'Studying the Internet experience', *HP LABORATORIES TECHNICAL REPORT HPL*, No. 49.

Burke, M, Marlow, C and Lento, T. Social network activity and social well-being. Proceedings of the SIGCHI conference on human factors in computing systems, 2010. ACM, 1909-1912.

Chapman, GB 1996, 'Temporal discounting and utility for health and money', *Journal of Experimental Psychology: Learning, Memory, and Cognition,* Vol. 22, No. 3**,** pp. 771.

Chretien, KC, Greysen, SR, Chretien, J-P*, et al.* 2009, 'Online posting of unprofessional content by medical students', *JAMA,* Vol. 302, No. 12**,** pp. 1309-1315.

Clark, JR 2010, 'Social media and privacy', *Air medical journal,* Vol. 29, No. 3**,** pp. 104-107.

Contena, B, Loscalzo, Y and Taddei, S 2015, 'Surfing on Social Network Sites: A comprehensive instrument to evaluate online self-disclosure and related attitudes', *Computers in Human Behavior,* Vol. 49**,** pp. 30-37.

Cronbach, LJ 1951, 'Coefficient alpha and the internal structure of tests', *psychometrika,* Vol. 16, No. 3**,** pp. 297-334.

Debatin, B, Lovejoy, JP, Horn, AK*, et al.* 2009, 'Facebook and online privacy: Attitudes, behaviors, and unintended consequences', *Journal of Computer-Mediated Communication,* Vol. 15, No. 1**,** pp. 83-108.

Deterding, S 2012, 'Gamification: designing for motivation', *interactions,* Vol. 19, No. 4**,** pp. 14-17.

Egelman, S and Peer, E. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015. ACM, 2873-2882.

Ellison, NB, Steinfield, C and Lampe, C 2007, 'The benefits of Facebook “friends:” Social capital and college students’ use of online social network sites', *Journal of Computer-Mediated Communication,* Vol. 12, No. 4**,** pp. 1143-1168.

Ellison, NB, Vitak, J, Steinfield, C*, et al.* 2011, *Negotiating privacy concerns and social capital needs in a social media environment*, Springer, 19-32.

Goodwin, C 1991, 'Privacy: Recognition of a consumer right', *Journal of Public Policy & Marketing***,** pp. 149-166.

Hull, G 2014, 'Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data', *Ethics and Information Technology***,** pp. 1-13.

Jiang, Z, Heng, CS and Choi, BC 2013, 'Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions', *Information Systems Research,* Vol. 24, No. 3**,** pp. 579-595.

Jones, H and Soltren, JH 2005, 'Facebook: Threats to privacy', *Project MAC: MIT Project on Mathematics and Computing,* Vol. 1**,** pp. 1-76.

Jones, S and Fox, S. 2009. Generations Online in 2009. Pew Internet & American Life Project, January 28, 2009, available at: http://www.pewInternet.org/~/media//Files/Reports/2009/PIP_Generations_2009.pdf (accessed 1/20/2016).

Katz, JE and Rice, RE 2002, *Social consequences of Internet use: Access, involvement, and interaction*, MIT press Cambridge, MA.

Kokolakis, S 2015, 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon', *Computers & Security*.

Kotz, D, Avancha, S and Baxi, A. A privacy framework for mobile health and home-care systems. Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems, 2009. ACM, 1-12.

Lampinen, A, Stutzman, F and Bylund, M. Privacy for a Networked World: bridging theory and design. CHI'11 Extended Abstracts on Human Factors in Computing Systems, 2011. ACM, 2441-2444.

Larsen, G and Lawson, R 2013, 'Consumer rights: an assessment of justice', *Journal of business ethics,* Vol. 112, No. 3**,** pp. 515-528.

Liberman, N, Sagristano, MD and Trope, Y 2002, 'The effect of temporal distance on level of mental construal', *Journal of experimental social psychology,* Vol. 38, No. 6**,** pp. 523-534.

Liberman, N, Trope, Y, Mccrea, SM*, et al.* 2007, 'The effect of level of construal on the temporal distance of activity enactment', *Journal of Experimental Social Psychology,* Vol. 43, No. 1**,** pp. 143-149.

Lutz, C and Strathoff, P 2014, 'Privacy Concerns and Online Behavior–Not so Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses'. *working paper.*

Mukhopadhyay, SC 2015, 'Wearable sensors for human activity monitoring: A review', *Sensors Journal, IEEE,* Vol. 15, No. 3**,** pp. 1321-1330.

Norberg, PA, Horne, DR and Horne, DA 2007, 'The privacy paradox: Personal information disclosure intentions versus behaviors', *Journal of Consumer Affairs,* Vol. 41, No. 1**,** pp. 100-126.

Park, S and Jayaraman, S 2003, 'Enhancing the quality of life through wearable technology', *Engineering in Medicine and Biology Magazine, IEEE,* Vol. 22, No. 3**,** pp. 41-48.

Patil, S, Patruni, B, Lu, H*, et al.* 2015, *Public Perception of Security and Privacy: Results of the comprehensive analysis of PACT's pan-European Survey*, RAND Corporation, Santa Monica, CA.

Petersen, C and Demuro, P 2015, 'Legal and Regulatory Considerations Associated with Use of Patient-Generated Health Data from Social Media and Mobile Health (mHealth) Devices', *Appl Clin Inform,* Vol. 6, No. 1**,** pp. 16-26.

Pew Research Center 2014, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center.

Piwek, L, Ellis, DA, Andrews, S*, et al.* 2015, 'The rise of consumer health wearables: promises and barriers', *PLoS Medicine*.

Shields, K 2015, 'Cybersecurity: Recognizing the Risk and Protecting against Attacks', *NC Banking Inst.,* Vol. 19**,** pp. 345.

Soghoian, C 2008, 'Exclusive: The next Facebook privacy scandal', *CNet News. Com*.

Solove, DJ 2008, 'Understanding privacy'.

Steinfield, C, Dimicco, JM, Ellison, NB*, et al.* Bowling online: social networking and social capital within the organization. Proceedings of the fourth international conference on Communities and technologies, 2009. ACM, 245-254.

Steinfield, C, Ellison, NB and Lampe, C 2008, 'Social capital, self-esteem, and use of online social network sites: A longitudinal analysis', *Journal of Applied Developmental Psychology,* Vol. 29, No. 6**,** pp. 434-445.

Topol, EJ, Steinhubl, SR and Torkamani, A 2015, 'Digital medical tools and sensors', *JAMA,* Vol. 313, No. 4**,** pp. 353-354.

Trope, Y and Liberman, N 2010, 'Construal-level theory of psychological distance', *Psychological review,* Vol. 117, No. 2**,** pp. 440.

Tufekci, Z 2008, 'Can you see me now? Audience and disclosure regulation in online social network sites', *Bulletin of Science, Technology & Society,* Vol. 28, No. 1**,** pp. 20-36.

Van Beek, J, Antonides, G and Handgraaf, MJ 2013, 'Eat now, exercise later: The relation between consideration of immediate and future consequences and healthy behavior', *Personality and Individual Differences,* Vol. 54, No. 6**,** pp. 785-791.

Viégas, FB 2005, 'Bloggers' expectations of privacy and accountability: An initial survey', *Journal of Computer-Mediated Communication,* Vol. 10, No. 3.

Xu, H, Luo, XR, Carroll, JM*, et al.* 2011, 'The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing', *Decision Support Systems,* Vol. 51, No. 1**,** pp. 42-52.

Xu, H, Teo, H-H, Tan, BC*, et al.* 2012, 'Research Note-Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services', *Information Systems Research,* Vol. 23, No. 4**,** pp. 1342-1363.