Digital Health and Social Needs: An Empirical Study of Intentions and Behaviors

Gianluca Zanella, Cory Hallam, Nasim Talebi
University of Texas at San Antonio, San Antonio, TX - USA

Abstract--**The convergence of wearable sensor technology and personalized predictive analytics has the potential to help researchers with early detection and treatment of medical problems. We anticipate that the clinical analysis of the flow of data coming from the individual's continuous monitoring will drive new discoveries and treatments. Moreover the development of personalized predictive models will drive the healthcare industry to shift from a reactive model to a proactive model, helping healthcare providers optimize care costs and offer a better customized service to patients. 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 the individuals' social habits. The convergence of social media with new wearable device features raises potential issues related to the online disclosure of sensitive medical data. Furthermore, the longitudinal collection of wearable data may lend itself to the development of new medical information, what we coin "emergent medical records". Data from an exploratory study shows how user intent to avoid potential privacy issues disclosing sensitive medical information collides with the individual's social propensity to share wearable information, generating a potentially regrettable behavior.**

I. RESEARCH PURPOSE

Progress in science and technology creates, as side effect, the potential for new 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 share the burden of recognizing and preventing potential issues arising from the progress in science and technology. The rise of social media is a perfect example how new technology that changed social behaviors all around the world 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 [24]. However, the growth in Social media has also highlighted the persistent, cumulative, and searchable nature of information, with unclear boundaries between public and private [45].

Privacy is a concern for many online social media users, but individual privacy attitudes are often inconsistent with behaviors. There is an ample literature about this gap, known as the privacy paradox [23]. As technology improves, new unexpected threats to privacy are exploited for online social networks. The charge for many scientists, experts, and policy makers is to recognize and mitigate these threats, and to educate people about it [16, 25, 47].

As the electronic industry has improved the production of miniaturized sensors, the prevalence of new devices designed to be worn on (and in) our bodies are multiplying fast [35]. These devices seamlessly collect, store, and transmit data, some of which could be considered as private and sensitive. While HIPAA rules apply for the storage and transmittal of medical information [33], 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.

Today, the most familiar devices include smart phone's apps coupled with smart bands, smart watches, and smart glasses, are 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 [6, 31, 42], providing researchers with extensive and accurate data, and offering clients personal health-care predictive analysis. However the concern is that the flow of highly sensitive data produced by wearable devices can be easily shared online through the social media networks. The main goal of this research is to address the gap between people's wearable privacy concerns (perceptions) and their real behavior.

II. ONLINE PRIVACY

The rise of online mediated-communication into the relationship development process has changed our lives, enabling individuals to connect synchronously with others and expand their circle of friends [21]. Research in the past decade shows that social capital [2] is a particularly significant outcome to consider when studying the use of social network sites [8, 14, 15, 38, 39]. The increased worldwide usage of smartphones and mobile devices has opened up the possibilities of individuals to share information with other 2 billion of users, creating an easy and attractive means to disseminate private, sensitive, and possibly inappropriate, harmful and even illegal information [9]. Given the persistent, cumulative, and searchable architecture of the World Wide Web, the private information and communications posted may be read for long time by everyone and constitute the "digital footprint" of an individual.

To address this growing problem, some countries have discussed and put into practice laws to establish a person's right to secure or erase potentially damaging, private information. Many countries have in practice laws to prevent and punish the misuse of online information. However the unclear boundaries of private versus public [22] creates a gap between the online privacy concerns about consequences of a breach of privacy, and the behavior of disclosing online personal information [45]. The gap between concerns and behavior, known as "privacy paradox" [7, 30], has been the focus of many studies [23], 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 [32, 34], but there is low correlation between privacy attitudes and online behavior [44]. The privacy paradox debate triggered research to explain this complex phenomenon through different theories and models, and brings into play the relationship between attitudes and behaviors.

A. Privacy attitudes and behavior

Current research is concerned to interpret the attitudes behavior dichotomy through different theories. The "Privacy Calculus Theory" proposes that behavior is a resulting balance between privacy concerns and social rewards [19, 46]. The 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 [28]. The Cognitive biases and heuristics in privacy decision-making draws from cognitive theory, proposing 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 the self-disclosure behavior [1]. Finally, the "Bounded rationality, incomplete information, and information asymmetries theory" proposes that the lack of knowledge constrains decisions. When people are provided context and knowledge, concerns are good predictors of intentions and behavior [1, 3].

While current research partially contributes to explaining some aspects of the privacy paradox, this complex phenomenon has not been fully explained [23]. Reviewing current theories interpreting this dichotomy, we note that two are based on the cognitive theory that the outcome is a balance between concerns and rewards, eventually moderated by biases and heuristics. Moreover the social theory proposes the outcome as a balance between more concrete immediate social rewards and more abstract distant-future social concerns. In the cognitive research literature the Construal Level Theory (CLT) [27, 43] shows how the choices people make every day are unconsciously based on a discounting process; near and positive outcomes weigh more than distant and negative outcomes in the personal evaluation of an action, because the distance discounts the negative aspects of that outcome. Combining these theories, we henceforth develop a more complete model that more accurately reflects the privacy paradox.

B. The Proposed Model

To create a better explanation of this complex phenomenon, we propose a theory based on a cognitive model (Fig. 1) that combines the current theories with the CLT perspective, in order 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) the risk-avoiding intention, which negatively affect the behavior, and 2) the trusting intention, which positively predicts the individual's self-disclosure. As Lutz and Strathoff [28] pointed out, 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 [28]. What is unclear if these perceptions hold given an individual's prior exposure to negative outcomes of the associated risks.

Construal Level Theory explains how any type of distance, social, temporal or psychological, impacts on our decision-making process. The positive value coming from a closer behavior is enhanced, while the negative value of a distant behavior is discounted [26, 27, 43]. 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 the breach of privacy, less value it will have on the choice of behavior. Therefore we expect that people with past experience with breach of privacy will give more value to the risk-avoiding intent. To identify the nature of the intention's antecedents, we draw from theories successfully applied in many others fields.

Over the last decades, medical and cognitive research has demonstrated that the extent to which individuals consider the future consequences of their behavior can have a significant effect on their choices [40]. The balance of immediate and future outcomes of a behavior affects the individual evaluation of the outcome and the consequent choice of behavior. In the context of our research, the future consequences of self-disclosing personal information are the probability of misuse of personal data, while the immediate consequences are the social rewards to feel part of a community sharing personal information. Consequently we propose that the consideration for future consequence (CFC_f) will positively affect the intentions to avoid the risk of misuse of personal information, while the consideration for immediate consequences (CFC_i) will affect positively the intentions to self-disclose personal data. As many other privacy-related theories state, privacy concerns are a strong predictor of the risk-avoiding intentions. On the opposite side, the social rewards are a predictor of the self-disclosing intentions [19, 28]. 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 [3], each with a different associated value [18].

C. Wearable devices

Medical research triggered the proliferation of small sensors that in the last few years has been used to make wearable device with the intent of monitoring individual's vital signs in real time. The first large-scale application of this new technology was fitness tracking devices, including smart bands, smart watches, some smart phone apps. The use of wearable sensor technology supports personalized predictive analytics to detect medical problems, which in turn will drive the healthcare to shift from a reactive model to a proactive model, helping the healthcare providers to optimize the costs and to offer a better customized service to their patients. The gamification [12] approach used to increase the sales of these new devices also pushes the social-reward side of the data flowing from the wearable technology, even though they may emerge with the potential to be used as healthcare data. Through the gamification lens, people are not made aware of the sensitive nature of the wearable data, exposing them to the potential misuse of this information.

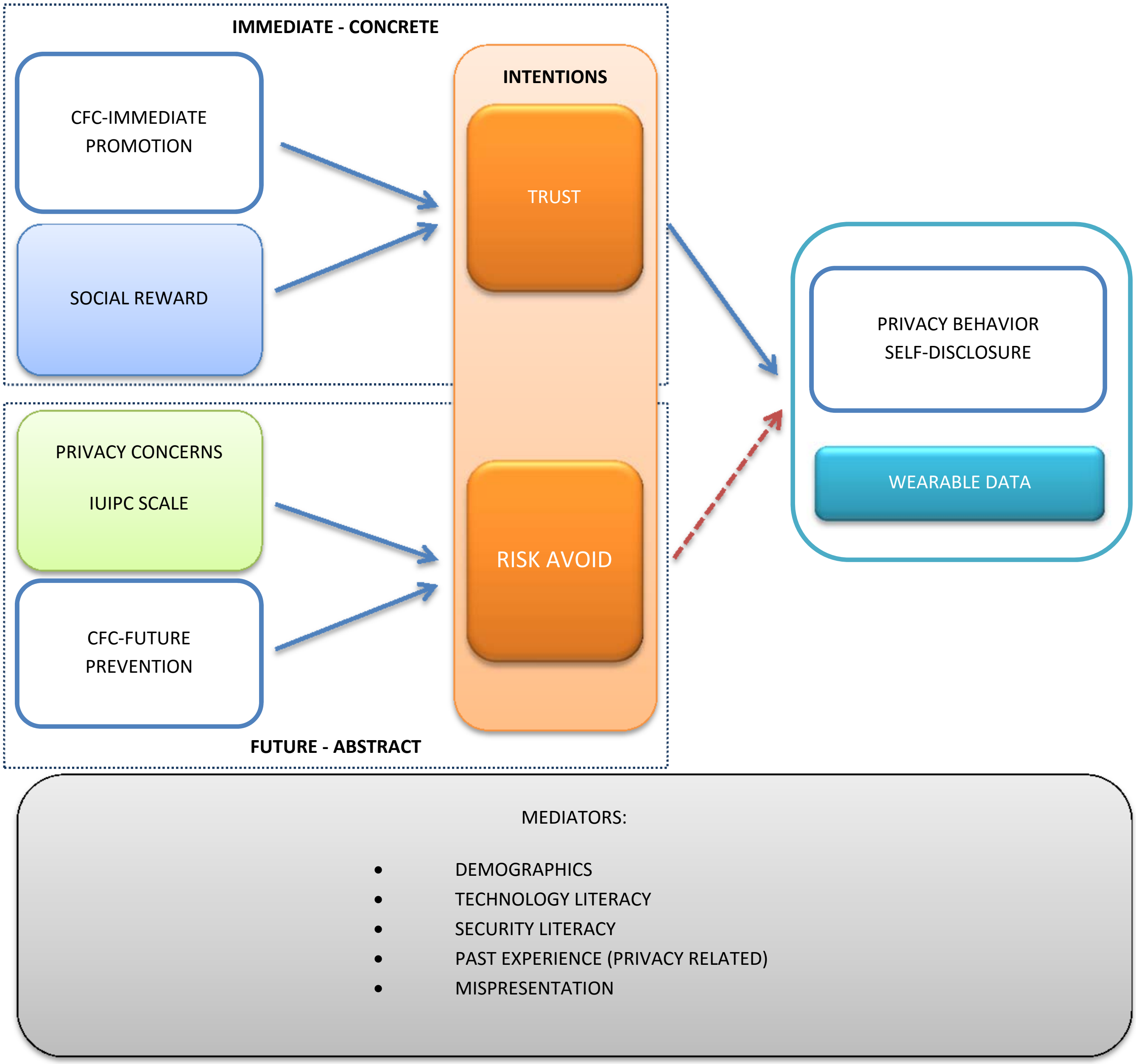

Figure 1. Proposed Model

III. RESEARCH METHOD AND ANALYSIS

A. Experiment design

A quasi-experimental exploratory study was designed to validate the proposed cognitive model that includes measures of intentions based on the Construal Level Theory. The instrument was an online survey administered with the snow-ball technique [4, 5]. The survey included a section to test the intention and the behavior of the users of wearable devices.

B. Measures

The Consideration of Future Consequences scale [20, 40] is the antecedent of the risk-avoiding intentions for the future factor, while it is antecedent of the self-disclosure intent through the immediate factor. The privacy attitudes are measured using the IUIPC scale [29]. The behaviors scale has been adapted from [19] and a new section has been developed for the wearable devices behavior, drawing from the Facebook behavior scale [10] and from the SeBIS security scale [13]. Each of these tools were previously validated.

C. Results

The preliminary sample was obtained with a snowball technique. The age of respondents was between 20 and 83, with the mean of 39.8. Forty two percent of respondents were male, and about 70% of the sample had a college degree. The average number of social media accounts per person was 3.5, and about 60% of our sample uses wearable devices or smart phone apps to track their daily activity. Table 1 reports the reliability coefficients for the instrument, including the Cronbach alpha [11] and the omega [36]. Moreover, we also checked for multicollinearity issues (see the Variance Inflation Factor in Table 1), and unidimensionality. The instrument performed discretely on the preliminary sample. The Long term Intentions and the Self-Disclosure Behavior could be reworded to achieve a better reliability, however we will track this further as the sample size is increased in the study.

TABLE1. CRONBACH ALPHA FOR THE LATENT VARIABLES

Latent Variable	Cronbach Alpha	Omega	VIF
CFC scale Future	0.85	0.85	< 2.2
CFC scale Immediate	0.88	0.88	< 4.1
Privacy Concerns (IUIPC)	0.90	0.90	< 4.6
Social Rewards	0.86	0.87	< 2.7
Self-disclosure Behavior	0.65	0.62	< 1.47
Long-term risk avoid Intentions	0.61	0.65	< 1.9
Short term self-disclosure Intentions	0.75	0.75	< 1.8

Given the small amount of data in our preliminary sample, we decided to test the proposed model using Partial Least Square Path Modeling (PLSPM) analysis [37]. Fig. 2 shows the outer model coefficients resulting from the PLSPM analysis on the preliminary data.

As expected, the Consideration about Future Consequences positively affects the long-term risk avoiding intentions, while the CFC Immediate positively affects the risk-avoiding intentions and negatively affects the self-disclosure intentions. Surprisingly the CFC Future exerts a positive effect on the self-disclosure Intentions, however with a small effect size. One possible explanation is that our model uses the CFC scale in his two-factor version, following the current research [20], instead of the original single-factor scale [40]. The CFC scale is a consistent and reliable instrument applied in many different fields [41], however there are still questions open about the optimal number of factors to consider in using that scale [17].

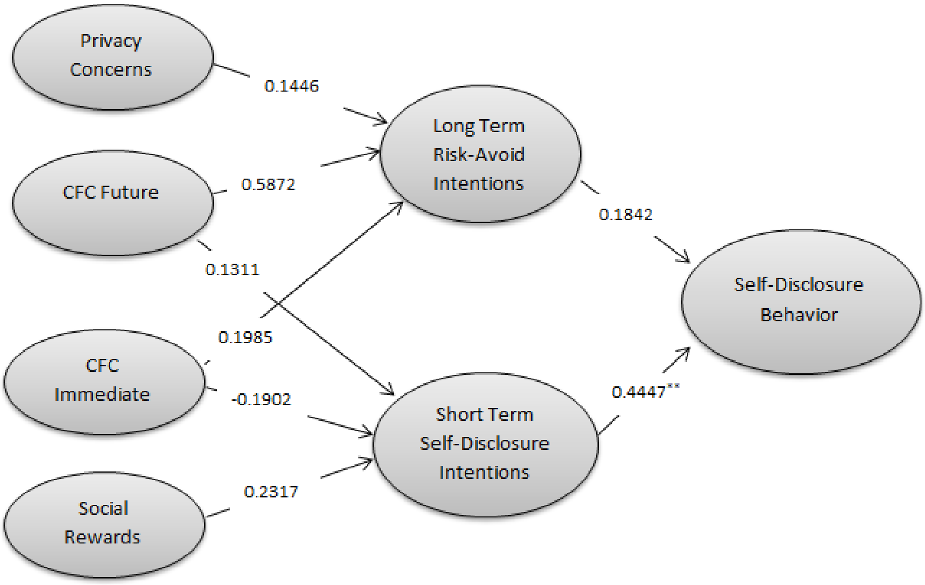

Figure 2. PLSPM results

Social rewards and Privacy concerns are respectively positively related to the self-disclosure intentions and to the risk-avoiding intentions. The short-term self-disclosure intentions exert a positive effect on the behavior, with a moderate to large effect size. Surprisingly, the long-term risk-avoiding intentions are positively related to the self-disclosure behavior, although with a small effect size. We expect that small inconsistencies in the analysis will be solved as more data is added to the sample. However 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. We expect, for example, that past negative experience and knowledge will increase the risk-avoiding effect on the individual's behavior.

IV. CONCLUSIONS

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

The Construal Level Theory (CLT) shows how the value of negative outcomes generated from abstract behaviors is discounted, while value of positive outcomes generated from concrete behaviors is enhanced. Our model, applying the CLT, shows that the intentions to avoid the abstract privacy risk are less related to the behavior than the concretely rewarding intentions to disclose personal information. This study is a step towards the explanation of the gap between privacy attitudes and behavior, which is crucial to preventing the tomorrows' privacy problems.

REFERENCES

[1] Acquisti, A. and J. Grossklags, "Privacy and rationality in individual decision making". *IEEE Security & Privacy*. vol. (1): pp. 26-33, 2005.

[2] Adler, P.S. and S.-W. Kwon, "Social capital: Prospects for a new concept". *Academy of management review*. vol. **27**(1): pp. 17-40, 2002.

[3] Baek, Y.M., "Solving the privacy paradox: A counter-argument experimental approach". *Computers in Human Behavior*. vol. **38**: pp. 33-42, 2014.

[4] Berg, S., "Snowball sampling—I". *Encyclopedia of statistical sciences*. vol., 1988.

[5] Biernacki, P. and D. Waldorf, "Snowball sampling: Problems and techniques of chain referral sampling". *Sociological methods & research*. vol. **10**(2): pp. 141-163, 1981.

[6] Bonato, P., "Wearable sensors/systems and their impact on biomedical engineering". *IEEE Engineering in Medicine and Biology Magazine*. vol. **22**(3): pp. 18-20, 2003.

[7] Brown, B., "Studying the Internet experience". *HP LABORATORIES TECHNICAL REPORT HPL*. vol. (49), 2001.

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

[9] Chretien, K.C., S.R. Greysen, J.-P. Chretien, and T. Kind, "Online posting of unprofessional content by medical students". *JAMA*. vol. **302**(12): pp. 1309-1315, 2009.

[10] Contena, B., Y. Loscalzo, and S. Taddei, "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, 2015.

[11] Cronbach, L.J., "Coefficient alpha and the internal structure of tests". *psychometrika*. vol. **16**(3): pp. 297-334, 1951.

[12] Deterding, S., "Gamification: designing for motivation". *interactions*. vol. **19**(4): pp. 14-17, 2012.

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

[14] Ellison, N.B., C. Steinfield, and C. Lampe, "The benefits of Facebook "friends:" Social capital and college students' use of online social network sites". *Journal of Computer‐Mediated Communication*. vol. **12**(4): pp. 1143-1168, 2007.

[15] Ellison, N.B., J. Vitak, C. Steinfield, R. Gray, and C. Lampe, "Negotiating privacy concerns and social capital needs in a social media environment", in *Privacy online*, Springer. p. 19-32. 2011.

[16] Goodwin, C., "Privacy: Recognition of a consumer right". *Journal of Public Policy & Marketing*. vol.: pp. 149-166, 1991.

[17] Hevey, D., et al., "Consideration of future consequences scale: Confirmatory factor analysis". *Personality and Individual Differences*. vol. **48**(5): pp. 654-657, 2010.

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

[19] Jiang, Z., C.S. Heng, and B.C. Choi, "Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions". *Information Systems Research*. vol. **24**(3): pp. 579-595, 2013.

[20] Joireman, J., M.J. Shaffer, D. Balliet, and A. Strathman, "Promotion orientation explains why future-oriented people exercise and eat healthy evidence from the two-factor consideration of future consequences-14 scale". *Personality and Social Psychology Bulletin*. vol. **38**(10): pp. 1272-1287, 2012.

[21] Jones, S. and S. Fox "Generations Online in 2009. Pew Internet & American Life Project, January 28, 2009",Retrieved 1/20/2016 World Wide Web, http://www.pewInternet.org/~/media//Files/Reports/2009/PIP_Generations_2009.pdf.

[22] Katz, J.E. and R.E. Rice, "Social consequences of Internet use: Access, involvement, and interaction". MIT press Cambridge, MA, 2002.

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

[24] Lampinen, A., F. Stutzman, and M. Bylund. "Privacy for a Networked World: bridging theory and design". in *CHI'11 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2011.

[25] Larsen, G. and R. Lawson, "Consumer rights: an assessment of justice". *Journal of business ethics*. vol. **112**(3): pp. 515-528, 2013.

[26] Liberman, N., M.D. Sagristano, and Y. Trope, "The effect of temporal distance on level of mental construal". *Journal of experimental social psychology*. vol. **38**(6): pp. 523-534, 2002.

[27] Liberman, N., Y. Trope, S.M. McCrea, and S.J. Sherman, "The effect of level of construal on the temporal distance of activity enactment". *Journal of Experimental Social Psychology*. vol. **43**(1): pp. 143-149, 2007.

[28] Lutz, C. and P. Strathoff, "Privacy Concerns and Online Behavior–Not so Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses". *Viewing the Privacy Paradox Through Different Theoretical Lenses (April 15, 2014)*. vol., 2014.

[29] Malhotra, N.K., S.S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model". *Information Systems Research*. vol. **15**(4): pp. 336-355, 2004.

[30] Norberg, P.A., D.R. Horne, and D.A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors". *Journal of Consumer Affairs*. vol. **41**(1): pp. 100-126, 2007.

[31] Park, S. and S. Jayaraman, "Enhancing the quality of life through wearable technology". *Engineering in Medicine and Biology Magazine, IEEE*. vol. **22**(3): pp. 41-48, 2003.

[32] Patil, S., et al., "Public Perception of Security and Privacy: Results of the comprehensive analysis of PACT's pan-European Survey", R. Corporation, Editor, RAND Corporation: Santa Monica, CA. 2015.

[33] Petersen, C. and P. DeMuro, "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**(1): pp. 16-26, 2015.

[34] PEW, "Public Perceptions of Privacy and Security in the Post-Snowden Era", Pew Research Center. 2014.

[35] Piwek, L., D.A. Ellis, S. Andrews, and A. Joinson, "The rise of consumer health wearables: promises and barriers". *PLoS Medicine*. vol., 2015.

[36] Revelle, W. and R.E. Zinbarg, "Coefficients alpha, beta, omega, and the glb: Comments on Sijtsma". *Psychometrika*. vol. **74**(1): pp. 145-154, 2009.

[37] Sanchez, G., "Understanding partial least squares path modeling with r". *Academic Paper Universitat Politècnica de Catalunya*. vol., 2009.

[38] Steinfield, C., J.M. DiMicco, N.B. Ellison, and C. Lampe. "Bowling online: social networking and social capital within the organization". in *Proceedings of the fourth international conference on Communities and technologies*. ACM, 2009.

[39] Steinfield, C., N.B. Ellison, and C. Lampe, "Social capital, self-esteem, and use of online social network sites: A longitudinal analysis". *Journal of Applied Developmental Psychology*. vol. **29**(6): pp. 434-445, 2008.

[40] Strathman, A., F. Gleicher, D.S. Boninger, and C.S. Edwards, "The consideration of future consequences: Weighing immediate and distant outcomes of behavior". *Journal of Personality and Social Psychology*. vol. **66**(4): pp. 742-752, 1994.

[41] Toepoel, V., "Is consideration of future consequences a changeable construct?". *Personality and Individual Differences*. vol. **48**(8): pp. 951-956, 2010.

[42] Topol, E.J., S.R. Steinhubl, and A. Torkamani, "Digital medical tools and sensors". *JAMA*. vol. **313**(4): pp. 353-354, 2015.

[43] Trope, Y. and N. Liberman, "Construal-level theory of psychological distance". *Psychological review*. vol. **117**(2): pp. 440, 2010.

[44] Tufekci, Z., "Can you see me now? Audience and disclosure regulation in online social network sites". *Bulletin of Science, Technology & Society*. vol. **28**(1): pp. 20-36, 2008.

[45] Viégas, F.B., "Bloggers' expectations of privacy and accountability: An initial survey". *Journal of Computer-Mediated Communication*. vol. **10**(3), 2005.

[46] Xu, H., X.R. Luo, J.M. Carroll, and M.B. Rosson, "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing". *Decision Support Systems*. vol. **51**(1): pp. 42-52, 2011.

[47] Xu, H., H.-H. Teo, B.C. Tan, and R. Agarwal, "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**(4): pp. 1342-1363, 2012.