Managing the gap between disruptive innovation and people's perceptions: the case of wearable devices

Gianluca Zanella* and Teja Guda

Center for Innovation, Technology, and Entrepreneurship,
The University of Texas at San Antonio,
San Antonio, TX 78249, USA
Email: gianluca.zanella@utsa.edu
Email: teja.guda@utsa.edu
*Corresponding author

Abstract: This study examines the relationship between social benefits, perceived risk, privacy assurance mechanisms, and self-disclosure of wearable devices data. Self-disclosure of wearable was hypothesised to be positively affected only by social benefits and not by perceived privacy risks. The findings of this study suggest that people perceive wearable devices as a new mean to interact with their social groups and not as a potential threat to their medical information. As expected, privacy concerns do not significantly affect the self-disclosure, while privacy assurance mechanisms do significantly affect self-disclosure. In addition, younger people are more likely to share online their wearable device's data. Given the sensitive nature of wearable device data, potential issues and concerns are discussed.

Keywords: wearable devices; privacy concerns; managing innovation; online self-disclosure; emerging medical records; technology intelligence and planning.

Reference to this paper should be made as follows: Zanella, G. and Guda, T. (2020) 'Managing the gap between disruptive innovation and people's perceptions: the case of wearable devices', *Int. J. Technology Intelligence and Planning*, Vol. 12, No. 4, pp.378–396.

Biographical notes: Gianluca Zanella is a Scientific Researcher at the Center for Innovation, Technology, and Entrepreneurship at the University of Texas at San Antonio. He is a technology entrepreneur. He has held various management positions throughout his career and has managed teams in Europe. His research interests include technology innovation, information technology, cyber security, and data analytics.

Teja Guda is an Assistant Professor at the Department of Biomedical Engineering, the University of Texas at San Antonio. Since 2014, the centre enables engineering and business students to form teams that develop and validate technology while simultaneously engaging in customer discovery towards the development of business plans for paths to market. He also manages the Innovation Lab, which is a rapid prototyping facility dedicated to teams working to take their technologies from lab to market. He revamped UTSA's biomedical engineering curriculum to include key concepts of customer discovery, technology commercialisation, and product design.

1 Introduction

Digital technologies have revolutionised the healthcare industry by improving the quality and accessibility of healthcare services. However, they have also posed serious privacy threats. The subsequent changes in the patient-physician relationship (McDonald, 1997) has enabled patients to access their electronic medical records (EMRs) in their desired time and format (Leroy and Dupuis, 2014). Apart from the traditional healthcare providers, a variety of new technologies also contribute to the creation and collection of medical data (Raghupathi and Raghupathi, 2014). Thanks to the recent advancements in telecommunications, sensor miniaturisation and data analysis technologies, healthcare monitoring systems are now embedded in many consumer accessories such as garments, hats, wrist bands, eyeglasses, wristwatches, headphones and smartphones (De Rossi et al., 2003; Patel et al., 2015; Zheng et al., 2014). The data collected by these systems are constantly uploaded on the cloud, creating a database of private and sensitive time-series data known as 'emergent medical records' (Hallam and Zanella, 2016). Unfortunately, the ubiquity of such sensors make them disappear in our daily lives and we use the info they provide without cautiously examining their medical nature (Gibson et al., 1979; Weiser, 1991). Therefore, the flow of emerging medical info goes unnoticed, merging with the increasing amount of data that our smart devices continuously generate. This, in turn, enables new potential threats to consumer's privacy (Arias et al., 2015; Chretien et al., 2009; Di Pietro and Mancini, 2003), which is at the core of this study:

> "The emerging form of medical records enabled by a new generation of sensors and data analytics technologies embedded in wearable devices facilitate new potential threats to consumer's privacy."

Users who are aware of the privacy risks associated with sharing sensitive data express concerns about their online privacy, often minimise their online info disclosure (Dinev et al., 2006b; Jiang et al., 2013) and use the available preventive measures (Dinev et al., 2006b; Jiang et al., 2013; Jones and Soltren, 2005; Taddicken, 2014; Tufekci, 2008). Besides, user's sense of possession or feeling of entitlement toward the wearable data trigger preventive measures that reduce the amount or the visibility of data shared online (Sharma and Crossler, 2014). Moreover, the presence of privacy assurance mechanisms, such as privacy assurance statements and privacy customisation options, improves the perceived trust on the wearable device vendor, which in turn favours online self-disclosure. However, the lack of consumer's awareness could cause the effect of the perceived risk associated with the use of these wearable devices to vanish altogether, thus leading to a potentially unsafe self-disclosure behaviour. The present explorative study try to address the following research question.

> "Are consumers aware of the sensitivity of the data created with wearable devices while they share such data with their online social circles?"

Our study seeks to investigate this question through a conceptual framework developed based on the constructs that were identified by the past literature, namely privacy assurance mechanisms, social benefits, perceived risk, and self-disclosure. The following section will discuss the theoretical background of our conceptual model.

2 Theoretical background

2.1 Self-disclosure

The integration of technologies in our daily lives increasingly drives users toward disclosure of their personal data. Self-disclosure refers to "what individuals voluntarily and intentionally reveal about themselves to others – including thoughts, feelings and experiences" (Posey et al., 2010). With more than 2 billion active users, smartphones and mobile devices have opened new possibilities for information sharing, leading to the dissemination of private, sensitive, and possibly inappropriate, harmful and even illegal information (Acquisti and Gross, 2006; Chretien et al., 2009). Disclosing personal information makes users vulnerable to various types of privacy risks, such as identity theft, loss of scholarship, or rejection of a job application (Barnes, 2006). However, people keep disclosing their information through social networks and infomediaries. Literature shows that disclosing information about the self is necessary in order to reap the benefits from online social interactions (Jozani et al., 2020). After all, members of one's social network cannot offer social support if they do not know it is needed (Ellison et al., 2011b). And online social network platforms leverage such needs by promoting the self-disclosure behaviour with an array of functional possibilities for sharing personal information across a large audience (Gross and Acquisti, 2005). The contrast between information privacy concerns and actual behaviour has been called the privacy paradox (Brown, 2001; Norberg et al., 2007). Past research proposes many theories to explain the gap between concerns and actions as the result of a trade-off (privacy calculus) between expected loss of privacy and the potential gain of disclosure (Dinev and Hart, 2006; Jiang et al., 2013; Xu et al., 2011). However, the privacy calculus alone is considered too simplistic and falls short in explaining why this problem extends to a wide portion of the population, including computer savvy people and IT professionals who do not lack this knowledge (Gordon, 2004; Kokolakis, 2017). To explain the contradicting findings related to user's social media behaviour, scholars have proposed irrational factors as moderators of the privacy calculus mechanism (Acquisti, 2004; Acquisti and Grossklags, 2003; Aivazpour and Rao, 2020; Blank et al., 2014; Hallam and Zanella, 2017).

In the case of healthcare data, the perceived high sensitivity of such data influences people's concerns about their privacy that, in turn, decreases their willingness to disclose online such information (Bansal and Gefen, 2010). Indeed, perceived privacy concerns negatively affect user's acceptance of online health information systems (ISs) (Grimes-Gruczka et al., 2000). The concerns are justified by many reasons. First, there is often discrepancy between policies and practices of online healthcare companies (Goldman et al., 2000). Second, national news report a growing number of data breaches related to medical information (Brubaker, 2000; Sullivan, 2000; Wahlberg, 1999). Finally, experts publicly agree that the number and diversity of third-party providers that need to access to patients electronic health records (EHRs) facilitates the possibility of data leakage, loss, or theft (Johnson, 2009). For these reasons, patients prefer to disclose less information and, at the same time, ask for more control over which health information should be shared with whom (Caine and Hanania, 2013). Furthermore, patients perceive the benefits of sharing their EHRs within the circle of clinical care but

still have considerable reservations about potential third-party access even if the information is de-identified. However, while progress in science and technology enables users to expand their circles of friends and acquaintances, at the same time it creates the potential for emergent issues and hazards. It is the case of wearable devices.

2.2 Wearable devices

The popularity of wearable devices increases rapidly, reflecting the introduction of new products such as smart glasses, smart watches, fitness and health trackers or even smart jewellery and smart fashion (Xu et al., 2012). The number of connected wearable devices worldwide is expected to increase from 325 million in 2014 to 929 million by 2021 (Cisco, 2017). Wearable devices are gadgets that are rapidly multiplying and can be worn or even implanted in human body with the aim of promoting and facilitating health behaviour changes among users. The most familiar gadgets are fitness trackers and smart watches monitoring health conditions and provide users/patients with complete access to online data services. Nevertheless, the potential of wearable devices depends significantly on the large amounts of data they generate and access. Since these devices can intermittently or continuously monitor and record relevant physiologic signals, they provide insights into new diagnostic and therapeutic avenues for patient care.

At the same time, a key issue concerning wearable devices arises from the amount of personal data they gather from their users. Since technology introduces greater uncertainty about who has access to information and how it is used, manufactures and service providers have placed greater attention on the terms of privacy assurance statements and privacy customisation features associated with wearable devices. However, examination of website policy disclosures has shown that privacy policies and adherence to them vary across industries (Culnan, 2000; Miyazaki and Fernandez, 2000). In a report written for nature, Austen (2015) identified that "when the Pew Research Center, an independent fact-gathering organisation in Washington DC, canvassed 1,600 experts in 2014 about the future of the internet, many expressed substantial concerns about privacy and people's abilities to control their own lives." Despite growing public concerns for information privacy, people increasingly use wearable devices (Smith et al., 2011; Xu et al., 2011).

Wearable device market players use very effective marketing strategies. First, they apply gamification design technique to create fun and engaging experiences, converting users into players. Second, they position their devices as personal mobile fitness coaches to motivate regular exercising by tracking the exercise quality and providing user feedback (Kranz et al., 2013). The regular use of the wearable devices maximises the positive outcomes of their functionality, thus creating trust among users and facilitating the embeddedness of these devices in user's daily life. According to utility theory, users' behaviours will reflect the most utilitarian attribute (Dinev and Hart, 2006). We propose that the marketing strategies that picture wearable devices as useful gadgets as well as the ubiquity of such devices in modern life may have lessen the perception of the sensitivity of data collected by these devices and have therefore increased self-disclosure behaviours. Our study seeks to investigate this conjecture through a conceptual framework developed based on the constructs that were identified by the past literature.

3 Research model and hypotheses

Medical information is among eight main categories of privacy research (Smith et al., 2011). Moreover, prior literature suggests that individuals are more concerned about their health information compared to any other types of personal information (Gostin and Nass, 2009; Kam and Chismar, 2005). Anderson and Agarwal (2011) suggest that "there is little else that is as consequential to an individual as his or her health information."

3.1 Privacy concerns

Privacy concerns is defined as "an individuals' concern about the threat to their information privacy when submitting their personal information on the Internet" (Bansal and Gefen, 2015; Son and Kim, 2008). ISs literature shows that privacy concerns influences intentions to purchase online (Malhotra et al., 2004), willingness to disclose sensitive personal information to create personal profiles (Culnan and Armstrong, 1999), and preferences for regulatory environments (Milberg et al., 2000). Consequently, individuals with high levels of privacy concerns may employ various privacy-protection responses to control the flow of sensitive information and minimise privacy-related risks (Son and Kim, 2008). Literature present empirical evidence that privacy concerns negatively affects the intent to self-disclose health information (Bansal and Gefen, 2010). Furthermore, Ellison et al. (2011a, 2011b) found a correlation between privacy concerns and a strategy of restricting online communication to select friends. However, such privacy-protection strategies negatively affect accruing social capital.

Privacy concerns affects self-disclosure intention in case of health data, however empirical studies on the relationship between self-disclosure and privacy concerns in several transactional situations, such as e-commerce and online shopping in general, online social network platforms, and finance services, have found no significant effects (Acquisti and Grossklags, 2005; Barnes, 2006; Beresford et al., 2012; Brown, 2001; Norberg et al., 2007; Taddicken, 2014; Tufekci, 2008; Zafeiropoulou, 2014). This confirms the peculiar nature of health information compared to any other types of personal information, since higher privacy concerns reflects perceived vulnerability and hence reduce patients' willingness to disclose private information (Gostin and Nass, 2009; Kam and Chismar, 2005). On the other hand, privacy concerns of users who do not consider wearable data as medical information do not affect self-disclosure. Thus, we propose:

H1 There is no significant relationship between privacy concerns and intention to self-disclose wearable devices data.

Past literature suggests that situational-specific factors such as social norms, perceived psychological ownership, and privacy assurance mechanisms affect the relationship between privacy concerns and self-disclosure. Therefore, we also include these interaction effects in our study.

3.2 Social norm

Social support is the main reason for users to engage in online self-disclosure (Ellison et al., 2007). This social interaction facilitates also the perception of belonging to a community with shared norms and values, which in turn influences the behaviour

(Clemens and Cook, 1999). Subjective norms or social influence refers to the extent to which user's decision making is influenced by others' perceptions (Sun et al., 2013; Venkatesh et al., 2003). The positive effect of social influence on the use and acceptance of technology such as e-government services and telemedicine technology has been empirically demonstrated (Hung et al., 2006). In their study of adoption of mobile health services Son and Kim (2008) found that there is a positive relationship between subjective norms and the use of mobile health services. Among all factors that affect an individual's intention to adopt healthcare wearable devices, social influence and perceived privacy risk are the most significant predictors. Consumers using healthcare wearable devices are more affected by others' behaviours and privacy concerns when it comes to manage their health conditions (Wang et al., 2015).

Few previous studies have disputed the relevance of social norms on self-disclosure behaviour, but only in workplaces and professional settings (Chau and Hu, 2001; Miltgen et al., 2013). For example, social influence does not play a significant role in health technology acceptance and use by professionals, because most professionals are certain about their decisions and are not worried about others' opinions (Chau and Hu, 2001). Furthermore, when new technologies do not affect social interaction, such as biometric authentication, factors such as trust in technology, concerns for data privacy, perceived risks and innovativeness are more relevant than subjective norms in predicting individual's behaviour (Miltgen et al., 2013). For the reasons explained above, any wearable healthcare technology implicates social interactions. Due to the growing frequency of using wearable devices and different mobile apps, along with many perceived benefits arising from using them, people are encouraging each other to adopt this technology. Therefore, we hypothesise that:

H2 There is a positive relationship between subjective norms and intention to self-disclose wearable devices data.

3.3 Perceived ownership

Perceived ownership is the feeling of possession and power about one's information (Furby, 1978a). The theoretical underpinnings of the psychological ownership concept has been thoroughly documented in the seminal works of Pierce et al. (2001), in which they highlight certain key features of this state. The first conceptual core of psychological ownership is the individual's sense of possession for an object. This sense of perceived ownership or sense of belongingness may also be experienced towards non-physical items such as ideas, personal information and the internet and would positively influence behavioural intention to protect these 'objects'. Second, psychological ownership is both cognitive and affective. In other words, it reflects an individual's awareness, thoughts, and beliefs regarding the target of possession and the associated personal meaning and emotion, or affect (Furby, 1978b). In this optic, the ultimate meaning of ownership is fusing the target of ownership with the self. Psychological (or perceived) ownership has emerged as an important predictor of motivations, attitudes, and behaviours (Jussila et al., 2015). As such, the users of wearable devices could associate the information to be shared online as their own as it provides them with sense of positivity, desirableness and self-identity. However, this perceived strong sense of ownership for their personal information push users to limit the impairment of it by restricting its access to third parties (Van Dyne and Pierce, 2004). Therefore, components of psychological ownership

theory have been recently adapted to marketing to successfully predict users' privacy concerns in disclosing personal information in social commerce environment (Sharma and Crossler, 2014). In agreement with the privacy concerns, literature provides empirical evidence that perceived ownership of personal information is one of the major motivators for the intentions to engage in behaviour related to protect personal information (Anderson and Agarwal, 2010). Thus, the more people have the feeling of possession or ownership of their information, the less likely they are willing to share and disclose them. Following our research question, we propose that people perceive wearable devices as gadgets, therefore they do not feel particular possession or ownership of wearable data. Consequently, we propose that:

H3 The relationship between perceived ownership and intention to self-disclose wearable devices data is not significant.

3.4 Moderating effect of privacy assurance mechanisms

Privacy assurance refers to "mechanisms that directly or indirectly provide customers with assurances and guarantees that their private information will be protected and kept private by the website" (Bansal and Gefen, 2015; Lowry et al., 2012). Privacy assurance mechanisms are among the most important website features for creating a trusted online environment which can be extended to the mobile apps offered by different developers along with wearable devices (Milne and Culnan, 2004). Having privacy assurance mechanisms in mind, wearable device users can protect themselves against threats of information disclosure (Bansal and Gefen, 2015). These mechanisms can be categorised into two main categories, namely privacy assurance statements and privacy customisation features (privacy assurance mechanisms in Figure 1).

Privacy assurance statements are communicated from app developers and wearable device designers to patients. They typically include statements about the adequacy of their protection measures (Bansal and Gefen, 2015). Research shows that when consumers understand that organisations have collected and used their personal information without their permission, their privacy concerns get triggered (Cespedes and Smith, 1993). However, consumers become less concerned about their privacy when organisations ask for permission to collect and use their information (Nowak and Phelps, 1995). Particularly, privacy assurance statement has a negative effect on privacy concerns by decreasing the susceptibility of privacy threat and increasing perceived effectiveness of assurance mechanisms. Therefore, if consumers are asked for permission and develop an understanding of what is going to be done with their data, the more protection they perceive from the privacy assurance statement the less they have privacy concerns. As a result, one can expect that privacy assurance mechanisms can play a vital role in decreasing the effect of consumers' privacy concerns on self-disclosure, leading to the following hypothesis:

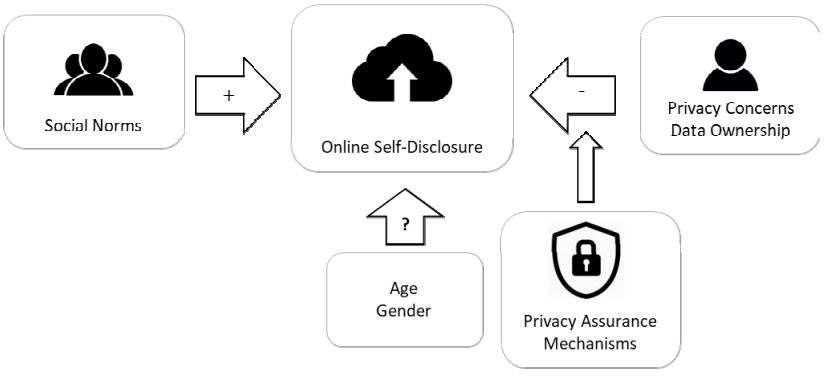
H4.1 Privacy assurance statement negatively affects the relationship between privacy concerns and intention to self-disclose wearable devices data.

Privacy customisation refers to consumers' efforts to use different features to change and control the flow of their information (Xu et al., 2011). Privacy customisation features have been studied in the context of social networking sites (Stutzman et al., 2011) and it has been found that privacy customisation features on SNSs do not have a significant

influence on users' assessment of the threat because there are several different tools such as web surfing tools and cookie management tools enabling users to protect themselves against privacy threats. However, when it comes to more sensitive information such as health information, individuals employ a 'pre-caution' strategy in order to protect themselves from threats (Maddux and Rogers, 1983). Likewise, individuals using wearable devices limit the access of others to their personal health information through which they have a perceived control over their information and, as a result, feel less vulnerable towards privacy threats. Therefore, apps or programs that let users customise their privacy preferences reduce the effect of user privacy concerns on self-disclosure, leading to the following hypothesis:

H4.2 Privacy customisation negatively affects the relationship between privacy concerns and intention to self-disclose wearable devices data.

Figure 1 Proposed model for the online self-disclosure of wearable data



4 Methodology

4.1 Research design and data collection

A quantitative study was designed to validate the research hypotheses depicted in Figure 1. The research instrument included seven-point Likert scale items that were adopted from measures already validated in the literature (see Table 1). Literature suggests that multiple linear regression requires a minimum sample size of 110 to achieve a power of 0.95 in detecting a medium effect size (Faul et al., 2009). Consequently, our goal was to obtain a sample size of at least 150 usable observations. The instrument used was an online survey administered to a convenience sample drawn from a population of students in a US public university. Participants in the initial sample were actual users of wearable devices enrolled in courses not specifically related to the topic of the research. Students were not rewarded course credits and the participation was voluntary and anonymous to avoid reactivity bias (Babbie, 2015).

The survey was taken by 190 individuals with the mean age of 26. 44% of respondents were female. 15% of surveyed students were using smartwatches to track their physiological factors, while the rest of the sample were using smart bands or smart

phone apps. Descriptive statistics and Pearson correlations for the sample are provided in Table 3.

Table 1 Scales used in the instrument

Self-disclosure intentions	Hallam and Zanella (2017)
Privacy concerns	Xu et al. (2011)
Privacy assurance statement	Xu et al. (2011)
Privacy customisation	Mousavizadeh and Kim (2015)
Perceived ownership	Van Dyne and Pierce (2004)
Social influence	Wu et al. (2012)

5 Results

5.1 Measurement model

An exploratory factor analysis (EFA) implemented with IBM SPSS 23.0 was conducted on 22 items. The Kaiser-Meyer-Olkin (KMO) index of sampling adequacy was good (KMO = 0.852). The Bartlett's test of sphericity was significant (χ^2 = 1,537.120, p = 0.000), indicating that we do have patterned relationships. Thus, our sample was suitable for EFA. Six components were extracted with an explained variance of 79.032 percent. Table 2 reports the EFA factor loadings after Promax rotation with Kaiser normalisation. Following previous literature, we dropped one items showing factor loadings smaller than 0.40 (Hinkin, 1998).

Table 2 EFA rotated factor matrix

	Factor					
	1	*2*	*3*	*4*	*5*	*6*
INTENT_1	–0.061	0.118	–0.032	0.083	–0.145	*0.774*
INTENT_2	0.014	0.054	0.073	–0.112	0.071	*0.710*
INTENT_3	0.085	–0.183	–0.024	0.026	0.106	*0.734*
CONCERN_1	0.043	*0.717*	0.084	–0.023	0.082	–0.036
CONCERN_2	0.040	*0.783*	–0.066	–0.006	0.035	0.019
CONCERN_3	0.005	*0.912*	–0.046	–0.016	–0.055	0.025
CONCERN_4	0.034	*0.892*	–0.004	0.008	–0.033	–0.018
OWNERSHIP_1	*0.824*	0.079	0.003	–0.024	0.036	0.075
OWNERSHIP_2	*0.999*	–0.005	–0.075	–0.004	–0.027	0.046
OWNERSHIP_3	*0.656*	0.033	0.100	0.111	0.091	–0.126
OWNERSHIP_4	*0.873*	–0.002	0.060	–0.023	–0.013	–0.019
OWNERSHIP_5	*0.920*	–0.019	0.004	0.027	–0.042	0.003
OWNERSHIP_6	0.242	–0.233	–0.167	–0.153	–0.147	–0.077
PRIV_ASS_1	0.072	–0.018	*0.813*	0.029	–0.055	0.033

Notes: Factor loadings > 0.4 are reported in ital. Promax rotation with Kaiser normalisation.

Table 2 EFA rotated factor matrix (continued)

	Factor					
	1	*2*	*3*	*4*	*5*	*6*
PRIV_ASS_2	0.007	–0.045	*0.950*	–0.031	–0.001	–0.019
PRIV_ASS_3	–0.007	0.036	*0.907*	–0.005	0.004	–0.005
PRIV_CUST_1	–0.006	–0.036	0.031	*0.914*	0.003	0.062
PRIV_CUST_2	0.041	0.021	–0.070	*0.906*	0.021	–0.035
PRIV_CUST_3	0.039	0.001	0.025	*0.842*	–0.030	–0.016
SUBJ_NORM_1	0.024	0.023	–0.041	0.001	*0.774*	0.033
SUBJ_NORM_2	0.037	0.006	–0.007	–0.039	*0.881*	–0.018
SUBJ_NORM_3	–0.043	–0.005	–0.005	0.031	*0.914*	–0.020

Notes: Factor loadings > 0.4 are reported in ital. Promax rotation with Kaiser normalisation.

Table 3 Internal reliability (alpha), CR, mean, standard deviation (SD), and Pearson correlation

		Alpha	*CR*	*Mean*	*SD*	*1*	*2*	*3*	*4*	*5*	*6*
1	Social norms	0.89	0.93	3.07	0.92						
2	P. ownership	0.85	0.91	5.06	1.20	0.22*					
3	Priv. concerns	0.90	0.93	4.28	1.50	0.35*	0.41*				
4	Priv. assurance	0.92	0.95	4.45	1.44	0.07	0.42*	0.18*			
5	Priv. customisation	0.92	0.95	4.74	1.60	0.17*	0.47*	0.35*	0.38*		
6	Self-disclosure	0.78	0.87	3.58	1.50	0.28*	–0.02	0.04	0.18*	–0.10	

Note: *significant at $p < 0.05$.

The reliability of each construct was assessed by analysing the Cronbach's alpha coefficient (Cronbach, 1951; Cronbach and Meehl, 1955) and the composite reliability (CR). Table 3 reports the reliability indexes and the Pearson correlations. Multicollinearity was not an issue because all the variance inflation factors (VIF) were smaller than three, well below the suggested limit of ten. Thus, the measurement model shows satisfactory reliability and validity.

5.2 Linear regression analysis

With the measurement validity largely established, we applied hierarchical linear regressions through R Software Version 3.2.3 for testing our hypotheses. Table 4 summarise the results from the regression models, also visualised in Figure 2. Model 1 is the baseline as it contains only control variables regressed over the sample. Gender do not significantly influence self-disclosure, while age is significantly predicting the intent to self-disclose wearable data throughout all the models ($\beta = –0.04$, $p < 0.005$). The younger the respondent, the higher the intention of self-disclose. Model 2 introduces the two main predictors of self-disclosure in our model, privacy concerns and social norms. As predicted in Hypothesis 1, privacy concerns do not significantly affect self-disclosure.

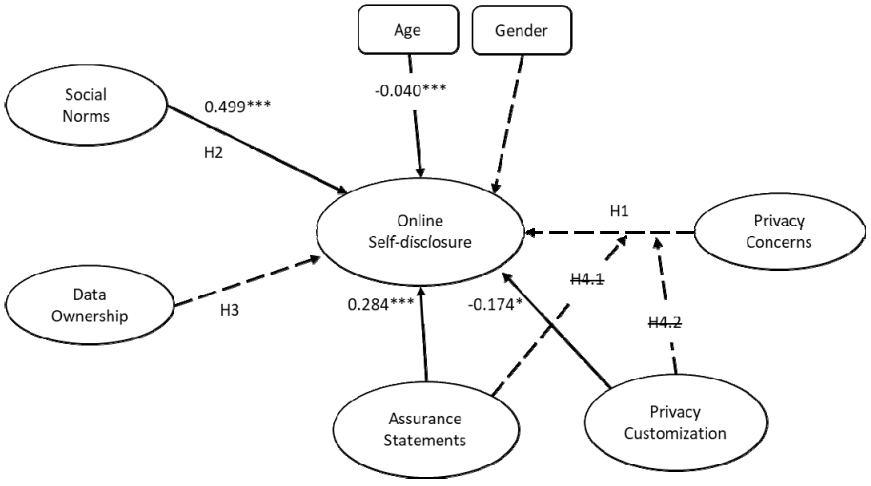
This is consistent with literature about the use of SNSs (Taddicken and Jers, 2011; Tufekci, 2008) and in general supports the existence of the privacy paradox (Kokolakis, 2017). Furthermore, this finding do not align with literature on self-disclosure of healthcare information (Gostin and Nass, 2009; Kam and Chismar, 2005), thus shredding light on the perceived leisure-oriented nature of these devices. Furthermore, social norms confirms to be a consistent and strong predictor of self-disclosure throughout all our models ($\beta = 0.499$, $p < 0.005$), thus confirming Hypothesis 2. Data ownership do not significantly predict self-disclosure, thus verifying Hypothesis 3. This finding confirms that respondents do not perceive the need to protect wearable information as they do in case of private or sensitive information (Anderson and Agarwal, 2010). Finally, we tested the moderating effect of privacy assurance mechanisms on self-disclosure.

Table 4 Hierarchical linear regression results for intention-based models

	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*
Social norms		0.479***	0.483***	0.499***	0.495***
Privacy concerns		–0.057	–0.046	–0.016	0.200
Data ownership			–0.037˙	–0.090	–0.128
Privacy assurance				0.284***	0.402*
Privacy customisation				–0.174*	–0.088
Age	–0.045***	–0.044***	–0.043***	–0.041***	–0.040***
Gender	–0.104	–0.122	–0.112	–0.074	–0.063
Concerns * assurance					–0.027
Concerns * customisation					–0.021
N	190	190	190	190	190
R squared	0.07	0.14	0.14	0.21	0.22
Intercept	4.899***	3.675***	3.770***	3.311***	2.591***

Notes: '***' $p < 0.001$; '**' $p < 0.01$; '*' $p < 0.05$; '.' $p < 0.1$.

Figure 2 Linear regression results



Privacy assurance statement do significantly affect self-disclosure, although with a sign opposite from what we predicted ($\beta = 0.284$, $p < 0.005$). One possible reason would be that users could perceive the privacy statement as adequate in order to feel that their privacy is protected, thus enabling more self-disclosure intention. This effect can be intensified in the case of highly private data, in which individuals are more sensitive to the adequacy and quality of the privacy statements. The interaction effect between privacy assurance and privacy concerns do not significantly affect the dependent variable, thus partially rejecting Hypothesis 4.1. The second privacy mechanism, customisation, do not affect the self-disclosure through the interaction with privacy concerns. Thus, we reject Hypothesis 4.2. However, privacy customisation does significantly affect the dependent variable ($\beta = –0.174$, $p < 0.05$). Offering privacy customisation makes our respondents less willing to self-disclose wearable data.

6 Conclusions

The pattern of our finding is consistent with the perceived nature of these devices, which is more oriented to leisure and fitness than to measuring medical data. Privacy is not a concern for users that intend to share wearable devices information with other people, which also confirms the social nature of this behaviour. These effects are consistent with the result of previous studies on user's self-disclosing behaviour on SNSs (Sun et al., 2013; Wang et al., 2015), as well as they are opposite to studies on disclosure of healthcare information, that have found privacy concerns to have negative impact on user's willingness to share information online (Tjora et al., 2005). Privacy assurance mechanisms have an intriguing effect on self-disclosure. Apparently, offering privacy customisation features to users make them more aware of possible threats, therefore increasing perceived threat susceptibility and concern about the privacy of their wearable data. Indeed, recent studies found that users find privacy choices as difficult to understand and utilise (Habib et al., 2020). On the other hand, privacy assurance statements apparently make people more confident and less concerned about their privacy. Finally, our findings related to privacy assurance mechanisms suggests that we can test their direct effect on self-disclosure, without the mediating effect of privacy concerns.

People are using health apps and wearable devices every day in order to track their activity and have a healthier life, but they are going to be more vulnerable to privacy intrusion by disclosing their personal health information. It has been shown that privacy practices are highly context-sensitive (Hull, 2014). As a result, we chose a growing and significant context like wearable devices measuring physiological factors thus generating healthcare-related data. The purpose of this study was to understand if users are aware of the sensitive nature of their wearable data. We have tried to answer this question by exploring factors affecting patients' self-disclosure behaviour in this context. Our findings provide evidence that users have not yet understood the sensitive nature of the data generated through wearable technology, therefore exposing themselves to potential privacy threats.

6.1 Contribution

This study makes a number of contributions. From a theoretical point of view, it reveals the process by which different privacy assurance mechanisms influence the privacy concerns and self-disclosure behaviour. Most previous studies have examined privacy assurance mechanisms in the context of e-commerce (Bansal and Gefen, 2015), where users are aware of the financial nature of the information exchanged. We apply this concept to the case of wearable devices, where the medical and sensitive nature of the information exchanged is not clearly disclosed. Indeed, the use of wearable data in lawsuits and criminal trials reflects such problem. Above all, our findings can provide insights for researchers developing particular applications to gather data from wearables. Of particular interest is the gap between the medical nature of wearable data and users' perceptions of such data. Such knowledge asymmetry between users' perceptions and data sensitivity offers an unregulated market to wearable manufacturers and, at the same time, provides a fertile ecosystem for the misuse and abuse of sensitive information. Future theoretical and applied research can take into account our results to study on the economic and security aspects of wearable devices. This research provides two main contributions relevant to practice and public policy. First, we provide evidence that the actual implementation of privacy customisation is not an appropriate mechanism to control user's concerns. This should inform website's designers on providing privacy customisation interfaces that support the users' perception of control and ownership over their sensitive data. In addition, policy makers should provide guidance on the design of privacy controls, thus leading to a standardisation of the set of privacy choices that, in turn, would allow users to develop consistent expectations and behaviours. Second, the perceived social and fitness-oriented nature of wearable data conceals the health-related core of such information, thus exposing the wearable users to serious privacy threats. Indeed, the marketing strategy of the various companies operating in this sector focuses on gamification and leisure as main features of their products. From our study, it is apparent that users are not aware of the medical nature of the data shared on the cloud, which is also gone under the radar of policy makers. Our findings contribute to raise the awareness on the sensitive nature of such data among regulators to prevent misuses and abuse of this emergent form of medical information. Finally, negative coverage by news outlets around the world can also affect the products adoption and diffusion dynamics (Marinakis et al., 2017). This should inform wearable manufacturers in re-orienting their communication strategy towards users' awareness.

6.2 Limitation and future research

Like many other studies, this study has limitations. First and foremost, this study is exploratory in nature, starting with a student sample limited to one university. Although university students represent a high percentage of mobile applications and wearable technology users, the use of a student sample might reduce the generalisability of our results. Future research should consider expanding the reach of the study through social media channels, aiming to collect data from a more diverse demographic and geographic sample. In addition, as it was suggested by Malhotra et al. (2004), future researchers can include sub-dimensions of privacy concerns such as control, collection, and awareness of privacy. Our current dataset lacks multi-national cultural diversity, which can be an influential factor since different cultures may care about privacy differently (Bellman

et al., 2004; Dinev et al., 2006a; Wu et al., 2012). Future studies may look at the differences in privacy concerns among different cultures in the context of wearable devices. Moreover, we only focused on self-disclosure intention. Future research should test our approach expanding the model to investigate the actual disclosure behaviour as the dependent variable.

References

Acquisti, A. (2004) 'Privacy in electronic commerce and the economics of immediate gratification', *Proceedings of the 5th ACM Conference on Electronic Commerce*, ACM, pp.21–29.

Acquisti, A. and Gross, R. (2006) 'Imagined communities: awareness, information sharing, and privacy on the Facebook', *Privacy Enhancing Technologies*, pp.36–58, Springer, Berlin, Heidelberg.

Acquisti, A. and Grossklags, J. (2003) 'Losses, gains, and hyperbolic discounting: an experimental approach to information security attitudes and behavior', *2nd Annual Workshop on Economics and Information Security-WEIS*, pp.1–27.

Acquisti, A. and Grossklags, J. (2005) 'Privacy and rationality in individual decision making', *IEEE Security & Privacy*, Vol. 3, No. 1, pp.26–33.

Aivazpour, Z. and Rao, V.S. (2020) 'Information disclosure and privacy paradox: the role of impulsivity', *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, Vol. 51, No. 1, pp.14–36.

Anderson, C.L. and Agarwal, R. (2010) 'Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions', *MIS Quarterly*, Vol. 34, No. 3, pp.613–643.

Anderson, C.L. and Agarwal, R. (2011) 'The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information', *Information Systems Research*, Vol. 22, No. 3, pp.469–490.

Arias, O., Wurm, J., Hoang, K. and Jin, Y. (2015) 'Privacy and security in internet of things and wearable devices', *IEEE Transactions on Multi-Scale Computing Systems*, Vol. 1, No. 2, pp.99–109.

Austen, K. (2015) 'The trouble with wearables', *Nature*, Vol. 525, No. 7567, p.22.

Babbie, E.R. (2015) *The Practice of Social Research*, Nelson Education, Belmont CA.

Bansal, G. and Gefen, D. (2010) 'The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online', *Decision Support Systems*, Vol. 49, No. 2, pp.138–150.

Bansal, G. and Gefen, D. (2015) 'The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern', *European Journal of Information Systems*, Vol. 24, No. 6, pp.624–644.

Barnes, S.B. (2006) 'A privacy paradox: social networking in the United States', *First Monday*, Vol. 11, No. 9, pp.1–6.

Bellman, S., Johnson, E.J., Kobrin, S.J. and Lohse, G.L. (2004) 'International differences in information privacy concerns: a global survey of consumers', *The Information Society*, Vol. 20, No. 5, pp.313–324.

Beresford, A.R., Kübler, D. and Preibusch, S. (2012) 'Unwillingness to pay for privacy: a field experiment', *Economics Letters*, Vol. 117, No. 1, pp.25–27.

Blank, G., Bolsover, G. and Dubois, E. (2014) *A New Privacy Paradox* [online] http://www.academia.edu/download/33687823/A_New_Privacy_Paradox_April_2014.pdf (accessed 20 November 2018).

Brown, B. (2001) 'Studying the internet experience', *HP Laboratories Technical Report HPL*, Vol. 49, No. 1, pp.1–23.

Brubaker, B. (2000) ''Sensitive' Kaiser e-mails go astray', *Washington Post*, Vol. 10, No. 1, pp.1–2.

Caine, K. and Hanania, R. (2013) 'Patients want granular privacy control over health information in electronic medical records', *Journal of the American Medical Informatics Association*, Vol. 20, No. 1, pp.7–15.

Cespedes, F.V. and Smith, H.J. (1993) 'Database marketing: new rules for policy and practice', *Sloan Management Review*, Vol. 34, No. 4, p.7.

Chau, P.Y. and Hu, P.J.H. (2001) 'Information technology acceptance by individual professionals: a model comparison approach', *Decision Sciences*, Vol. 32, No. 4, pp.699–719.

Chretien, K.C., Greysen, S.R., Chretien, J-P. and Kind, T. (2009) 'Online posting of unprofessional content by medical students', *JAMA*, Vol. 302, No. 12, pp.1309–1315.

Cisco (2017) 'Cisco visual networking index: global mobile data traffic forecast update 2016–2021', *Cisco Public Information*, 7 February 7.

Clemens, E.S. and Cook, J.M. (1999) 'Politics and institutionalism: explaining durability and change', *Annual Review of Sociology*, Vol. 25, No. 1, pp.441–466.

Cronbach, L.J. (1951) 'Coefficient alpha and the internal structure of tests', *Psychometrika*, Vol. 16, No. 3, pp.297–334.

Cronbach, L.J. and Meehl, P.E. (1955) 'Construct validity in psychological tests', *Psychological Bulletin*, Vol. 52, No. 4, p.281.

Culnan, M.J. (2000) 'Protecting privacy online: is self-regulation working?', *Journal of Public Policy & Marketing*, Vol. 19, No. 1, pp.20–26.

Culnan, M.J. and Armstrong, P.K. (1999) 'Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation', *Organization Science*, Vol. 10, No. 1, pp.104–115.

De Rossi, D., Carpi, F., Lorussi, F., Mazzoldi, A., Paradiso, R., Scilingo, E.P. and Tognetti, A. (2003) 'Electroactive fabrics and wearable biomonitoring devices', *AUTEX Research Journal*, Vol. 3, No. 4, pp.180–185.

Di Pietro, R. and Mancini, L.V. (2003) 'Security and privacy issues of handheld and wearable wireless devices', *Communications of the ACM*, Vol. 46, No. 9, pp.74–79.

Dinev, T. and Hart, P. (2006) 'An extended privacy calculus model for e-commerce transactions', *Information Systems Research*, Vol. 17, No. 1, pp.61–80.

Dinev, T., Bellotto, M., Hart, P., Russo, V. and Serra, I. (2006a) 'Internet users' privacy concerns and beliefs about government surveillance: an exploratory study of differences between Italy and the United States', *Journal of Global Information Management*, Vol. 14, No. 4, pp.57–93.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. (2006b) 'Privacy calculus model in e-commerce – a study of Italy and the United States', *European Journal of Information Systems*, Vol. 15, No. 4, pp.389–402.

Ellison, N.B., Lampe, C., Steinfield, C. and Vitak, J. (2011a) 'With a little help from my friends: how social network sites affect social capital processes', *The Networked Self: Identity, Community and Culture on Social Network Sites*, pp.124–146, Routledge, New York, NY.

Ellison, N.B., 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, N.B., Vitak, J., Steinfield, C., Gray, R. and Lampe, C. (2011b) 'Negotiating privacy concerns and social capital needs in a social media environment', in *Privacy Online*, pp.19–32, Springer, Berlin, Heidelberg.

Faul, F., Erdfelder, E., Buchner, A. and Lang, A-G. (2009) 'Statistical power analyses using G* Power 3.1: tests for correlation and regression analyses', *Behavior Research Methods*, Vol. 41, No. 4, pp.1149–1160.

Furby, L. (1978a) 'Possession in humans: an exploratory study of its meaning and motivation', *Social Behavior and Personality: An International Journal*, Vol. 6, No. 1, pp.49–65.

Furby, L. (1978b) 'Possessions: toward a theory of their meaning and function throughout the life cycle', in Baltes, P.B. (Ed.): *Life-Span Development and Behavior*, pp.297–336, Academic Press, New York.

Gibson, E.J., Owsley, C.J., Walker, A. and Megaw-Nyce, J. (1979) 'Development of the perception of invariants: substance and shape', *Perception*, Vol. 8, No. 6, pp.609–619.

Goldman, J., Hudson, Z. and Smith, R. (2000) *Privacy: Report on the Privacy Policies and Practices of Health Web Sites*, California Healthcare Foundation, Oakland, CA.

Gordon, S. (2004) *Privacy: A Study of Attitudes and Behaviors in US, UK and EU Information Security Professionals*, Symantec White Paper.

Gostin, L.O. and Nass, S. (2009) 'Reforming the HIPAA privacy rule: safeguarding privacy and promoting research', *JAMA*, Vol. 301, No. 13, pp.1373–1375.

Grimes-Gruczka, T., Gratzer, C. and Dialogue, C. (2000) *Ethics: Survey of Consumer Attitudes About Health Web Sites*, California Healthcare Foundation.

Gross, R. and Acquisti, A. (2005) 'Information revelation and privacy in online social networks', *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, ACM, pp.71–80.

Habib, H., Pearman, S., Wang, J., Zou, Y., Acquisti, A., Cranor, L.F., Sadeh, N. and Schaub, F. (2020) ''It's a scavenger hunt': usability of websites' opt-out and data deletion choices', *CHI*.

Hallam, C. and Zanella, G. (2016) 'Wearable device data and privacy: a study of perception and behavior', *World Journal of Management*, Vol. 7, No. 1, pp.82–91.

Hallam, C. and Zanella, G. (2017) 'Online self-disclosure: the privacy paradox explained as a temporally discounted balance between concerns and rewards', *Computers in Human Behavior*, Vol. 68, No. 2017, pp.217–227.

Hinkin, T.R. (1998) 'A brief tutorial on the development of measures for use in survey questionnaires', *Organizational Research Methods*, Vol. 1, No. 1, pp.104–121.

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*, Vol. 17, No. 2, pp.1–13.

Hung, S-Y., Chang, C-M. and Yu, T-J. (2006) 'Determinants of user acceptance of the e-government services: the case of online tax filing and payment system', *Government Information Quarterly*, Vol. 23, No. 1, pp.97–122.

Jiang, Z., Heng, C.S. and Choi, B.C. (2013) 'Research note – privacy concerns and privacy-protective behavior in synchronous online social interactions', *Information Systems Research*, Vol. 24, No. 3, pp.579–595.

Johnson, M.E. (2009) 'Data hemorrhages in the health-care sector', *International Conference on Financial Cryptography and Data Security*, Springer, pp.71–89.

Jones, H. and Soltren, J.H. (2005) 'Facebook: threats to privacy', *Project MAC: MIT Project on Mathematics and Computing*, Vol. 1, No. 1, pp.1–76.

Jozani, M., Ayaburi, E., Ko, M. and Choo, K-K.R. (2020) 'Privacy concerns and benefits of engagement with social media-enabled apps: a privacy calculus perspective', *Computers in Human Behavior*, Vol. 107, No. 2020, p.106260.

Jussila, I., Tarkiainen, A., Sarstedt, M. and Hair, J.F. (2015) 'Individual psychological ownership: concepts, evidence, and implications for research in marketing', *Journal of Marketing Theory and Practice*, Vol. 23, No. 2, pp.121–139.

Kam, L.E. and Chismar, W.G. (2005) 'Online self-disclosure: model for the use of internet-based technologies in collecting sensitive health information', *International Journal of Healthcare Technology and Management*, Vol. 7, Nos. 3–4, pp.218–232.

Kokolakis, S. (2017) 'Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon', *Computers & Security*, Vol. 64, No. 2017, pp.122–134.

Kranz, M., Möller, A., Hammerla, N., Diewald, S., Plötz, T., Olivier, P. and Roalter, L. (2013) 'The mobile fitness coach: towards individualized skill assessment using personalized mobile devices', *Pervasive and Mobile Computing*, Vol. 9, No. 2, pp.203–215.

Leroy, M.C. and Dupuis, M. (2014) 'Patients' direct access to their electronic medical record using the internet: a literature review', *Ramon Llull Journal of Applied Ethics*, Vol. 1, No. 5, pp.9–22.

Lowry, P.B., Moody, G., Vance, A., Jensen, M., Jenkins, J. and Wells, T. (2012) 'Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers', *Journal of the American Society for Information Science and Technology*, Vol. 63, No. 4, pp.755–776.

Maddux, J.E. and Rogers, R.W. (1983) 'Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change', *Journal of Experimental Social Psychology*, Vol. 19, No. 5, pp.469–479.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004) 'Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model', *Information Systems Research*, Vol. 15, No. 4, pp.336–355.

Marinakis, Y., Harms, R., Ahluwalia, S. and Walsh, S.T. (2017) 'Explaining product adoption and diffusion at the base of the pyramid', *International Journal of Technology Intelligence and Planning*, Vol. 11, No. 4, pp.345–365.

McDonald, C.J. (1997) 'The barriers to electronic medical record systems and how to overcome them', *Journal of the American Medical Informatics Association*, Vol. 4, No. 3, pp.213–221.

Milberg, S.J., Smith, H.J. and Burke, S.J. (2000) 'Information privacy: corporate management and national regulation', *Organization Science*, Vol. 11, No. 1, pp.35–57.

Milne, G.R. and Culnan, M.J. (2004) 'Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices', *Journal of Interactive Marketing*, Vol. 18, No. 3, pp.15–29.

Miltgen, C.L., Popovič, A. and Oliveira, T. (2013) 'Determinants of end-user acceptance of biometrics: integrating the 'big 3' of technology acceptance with privacy context', *Decision Support Systems*, Vol. 56, pp.103–114.

Miyazaki, A.D. and Fernandez, A. (2000) 'Internet privacy and security: an examination of online retailer disclosures', *Journal of Public Policy & Marketing*, Vol. 19, No. 1, pp.54–61.

Mousavizadeh, M. and Kim, D. (2015) 'A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of protection motivation theory', *ICIS 2015 Proceedings*.

Norberg, P.A., Horne, D.R. and Horne, D.A. (2007) 'The privacy paradox: personal information disclosure intentions versus behaviors', *Journal of Consumer Affairs*, Vol. 41, No. 1, pp.100–126.

Nowak, G.J. and Phelps, J. (1995) 'Direct marketing and the use of individual-level consumer information: determining how and when 'privacy' matters', *Journal of Direct Marketing*, Vol. 9, No. 3, pp.46–60.

Patel, M.S., Asch, D.A. and Volpp, K.G. (2015) 'Wearable devices as facilitators, not drivers, of health behavior change', *JAMA*, Vol. 313, No. 5, pp.459–460.

Pierce, J.L., Kostova, T. and Dirks, K.T. (2001) 'Toward a theory of psychological ownership in organizations', *Academy of Management Review*, Vol. 26, No. 2, pp.298–310.

Posey, C., Lowry, P.B., Roberts, T.L. and Ellis, T.S. (2010) 'Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities', *European Journal of Information Systems*, Vol. 19, No. 2, pp.181–195.

Raghupathi, W. and Raghupathi, V. (2014) 'Big data analytics in healthcare: promise and potential', *Health Information Science and Systems*, Vol. 2, No. 1, p.3.

Sharma, S. and Crossler, R.E. (2014) 'Disclosing too much? Situational factors affecting information disclosure in social commerce environment', *Electronic Commerce Research and Applications*, Vol. 13, No. 5, pp.305–319.

Smith, H.J., Dinev, T. and Xu, H. (2011) 'Information privacy research: an interdisciplinary review', *MIS Quarterly*, Vol. 35, No. 4, pp.989–1016.

Son, J-Y. and Kim, S.S. (2008) 'Internet users' information privacy-protective responses: a taxonomy and a nomological model', *MIS Quarterly*, Vol. 32, No. 3, pp.503–529.

Stutzman, F., Capra, R. and Thompson, J. (2011) 'Factors mediating disclosure in social network sites', *Computers in Human Behavior*, Vol. 27, No. 1, pp.590–598.

Sullivan, B. (2000) *Bank Information Exposed Online*, MSNBC.

Sun, Y., Wang, N., Guo, X. and Peng, Z. (2013) 'Understanding the acceptance of mobile health services: a comparison and integration of alternative models', *Journal of Electronic Commerce Research*, Vol. 14, No. 2, p.183.

Taddicken, M. (2014) 'The 'privacy paradox' in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure', *Journal of Computer-Mediated Communication*, Vol. 19, No. 2, pp.248–273.

Taddicken, M. and Jers, C. (2011) 'The uses of privacy online: trading a loss of privacy for social web gratifications?', in *Privacy Online*, pp.143–156, Springer, Berlin, Heidelberg.

Tjora, A., Tran, T. and Faxvaag, A. (2005) 'Privacy vs. usability: a qualitative exploration of patients' experiences with secure internet communication with their general practitioner', *Journal of Medical Internet Research*, Vol. 7, No. 2, p.e15.

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 Dyne, L. and Pierce, J.L. (2004) 'Psychological ownership and feelings of possession: three field studies predicting employee attitudes and organizational citizenship behavior', *Journal of Organizational Behavior*, Vol. 25, No. 4, pp.439–459.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003) 'User acceptance of information technology: toward a unified view', *MIS Quarterly*, Vol. 27, No. 3, pp.425–478.

Wahlberg, D. (1999) 'Patient records exposed on web', *Ann Arbor News*, Vol. 10, No. 1, p.1.

Wang, P.L.W.X., Chen, D.X., Gao, Y., Li, H. and Luo, Y. (2015) 'An empirical study of wearable technology acceptance in healthcare', *Industrial Management & Data Systems*, Vol. 115, No. 9, pp.1704–1723.

Weiser, M. (1991) 'The computer for the 21st century', *Scientific American*, Vol. 265, No. 3, pp.94–104.

Wu, K-W., Huang, S.Y., Yen, D.C. and Popova, I. (2012) 'The effect of online privacy policy on consumer privacy concern and trust', *Computers in Human Behavior*, Vol. 28, No. 3, pp.889–897.

Xu, H., Dinev, T., Smith, J. and Hart, P. (2011) 'Information privacy concerns: linking individual perceptions with institutional privacy assurances', *Journal of the Association for Information Systems*, Vol. 12, No. 12, p.798.

Xu, H., Teo, H-H., Tan, B.C. and Agarwal, R. (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.

Zafeiropoulou, A-M. (2014) *A Paradox of Privacy: Unravelling The Reasoning Behind Online Location Sharing*, University of Southampton.

Zheng, Y-L., Ding, X-R., Poon, C.C.Y., Lo, B.P.L., Zhang, H., Zhou, X-L., Yang, G-Z., Zhao, N. and Zhang, Y-T. (2014) 'Unobtrusive sensing and wearable devices for health informatics', *IEEE Transactions on Biomedical Engineering*, Vol. 61, No. 5, pp.1538–1554.

Appendix

The instrument

Social influence	SUBJ_NORM_1	People who are important to me would think that I should use wearable devices.
	SUBJ_NORM_2	People who influence would think that I should use wearable devices.
	SUBJ_NORM_3	People whose opinions are valued to me would prefer that I should use wearable devices.
Wearable intention to disclose	INTENT_1	If my friends gave me a new model of wearable device, I would openly share the data online.
	INTENT_2	If my employer gave me a new model of wearable device, I would share my activity data with the employer.
	INTENT_3	To obtain a free gift valued at $50, I would share my activity data online.
Wearable concerns	CONCERN_1	The information I submit to this wearable device could be misused.
	CONCERN_2	Others can find private information about me from this wearable device.
	CONCERN_3	I am concerned because of what others might do with it.
	CONCERN_4	I am concerned because it could be used in a way I did not foresee.
Perceived ownership	OWNERSHIP_1	The health information I share via wearable devices is MY personal information.
	OWNERSHIP_2	I sense that the health information I provide via wearable devices is my own.
	OWNERSHIP_3	I feel a very high degree of personal ownership for health information I provide via wearable devices.
	OWNERSHIP_4	I sense that the health information I provide via wearable devices is personal.
	OWNERSHIP_5	I believe that the health information I disclose via wearable devices belongs to me.
	OWNERSHIP_6	It is hard for me to think about the health information I disclose via wearable devices as MINE.
Privacy assurance	PRIV_ASS_1	I feel confident that wearable devices' privacy assurance statements reflect their commitments to protect my personal health information.
	PRIV_ASS_2	With their privacy assurance statements, I believe that my personal health information will be kept private and confidential.
	PRIV_ASS_3	I believe that wearable devices' privacy assurance statements are an effective way to demonstrate their commitments to privacy.
Privacy customisation	PRIV_CUST_1	I customise my wearable device privacy settings when I share my health information.
	PRIV_CUST_2	I prefer to customise privacy settings of my wearable device before I share my health information.
	PRIV_CUST_3	I usually use privacy customisation feature.