An Exploratory Survey of the Effects of Perceived Control and Perceived Risk on Information Privacy

Clare Doherty and Dr. Michael Lang
Business Information Systems Department, JE Cairnes School of Business & Economics
National University of Ireland Galway
County Galway, Ireland
{c.doherty2, michael.lang}@nuigalway.ie

***Abstract*—The purpose of this research is to investigate two factors that affect a user's information privacy online. An exploratory survey was conducted in Ireland receiving 260 usable responses. Users' attitudes and behaviors toward information privacy were explored in relation to a user's level of perceived control and perceived risk. The preliminary findings show that the more control users have, the more information they will disclose, and that the more risk they perceive, the less information they will disclose online. These findings have provided the basis for further analysis to better understand the effect of these two factors on information disclosure when engaging in online activities.**

Keywords—Perceived Risk; Perceived Control; Online Disclosure; Information Privacy

I. INTRODUCTION

Information privacy concern refers to the extent to which a user perceives they have control over their personal information and whether they have knowledge of the use/exchange of this information [1]. Information privacy is a concern for the majority of internet users, from consumers to e-businesses. In a recent poll conducted on behalf of the Computer and Communications Industry Association (CCIA), 75% of respondents are worried that information disclosed by them online will be used to cause harm or steal from them [2]. In January 2014 it was claimed that 70% of people living in Ireland have suffered a violation of privacy [3]. The media has reported a number of high profile online privacy breaches in recent times including the Apple iPhone tracking controversy [4], the Sony PlayStation Network break-in which compromised the details of over 75 million users [5] and the theft of personal data of over 1.5 million European customers at Loyaltybuild [6]. These and other cases are raising public awareness and concerns as regards privacy breaches, which may lead to more cautious online behavior and an increased reluctance to reveal personal information online. That however is a matter of speculation so this study, building upon the previous research of Belanger & Crossler [7] and Smith et al. [8], sets out to improve our understanding of how perceived control and perceived risk affect information disclosure (i.e. revealing information about oneself online), taking into consideration an individual's privacy concerns, trust disposition, risk propensity, and prior negative experiences if any. An exploratory survey was our chosen approach, the aim being to seek out interesting findings which would then be investigated more closely with a follow-up study.

Our research-in-progress paper is organized as follows: Section II briefly outlines the theory and literature review. Section III provides the research method. Section IV presents the initial findings and Section V provides the conclusion and future research.

II. THEORETICAL BACKGROUND & LITERATURE REVIEW

In their systematic review of information privacy research, Belanger and Crossler [7] state that risk and control are not as frequently researched as other factors. Smith et al. [8] make the point that research should focus on outcomes associated with information privacy concerns at the individual level of analysis because it is an under-researched area. As established in a number of previous studies, perceived control is positively correlated to information disclosure [9], [10], [11], [12], [13] and perceived risk is negatively correlated to information disclosure [14], [15], [16], [17], [18]. Where our work differs from that of previous authors is in its focus on perceived risk and control in so far as they relate to information privacy concerns.

A. Perceived Control

Privacy has been defined as the "representation of the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimize vulnerability" [19]. This concept of privacy has been associated with the psychological/personal control over information [20]. People may have an illusion of control over events e.g., disclosure behavior, which actually may in fact be uncontrollable [21]. Control influences and is influenced by the situation; for example, disclosing information when partaking in online activities. Therefore it is an important variable when considering privacy, being central to Westin and Altman's theories of privacy [22], [23].

It has been argued that privacy invasion is caused by the loss of control over personal information [24]. Trust is viewed as a significant factor in the reduction of perceived risk when disclosing information online; however trust is itself dependent upon the ability to control the behavior of others [25]. A lack of trust can develop when users perceive a lack of control over

the information online sites gather about them [26]. Internet users possess a low level of trust in online companies if they perceive themselves as having little or no control over what these online companies do with their personal information once it is disclosed [26]. In the information privacy context, consumers take high risks in the disclosure of personal information online which puts greater importance on a user's perceived control. Therefore there is greater interest required to be given by companies to promote privacy awareness for users (e.g., use of privacy-protecting technologies) and for users to become more experienced with these technologies. Once users become more proficient with these privacy tools they will become more confident, thus reducing the chances that they will become the victim of unauthorized access or personal information misuse online. This will lead to greater control and trust that users will perceive themselves to possess, which in turn leads to greater online participation [17], [27]. However, users must bear in mind, as Netchitailova [28] states, that "connecting with people always means giving up some control over your personal details: 'Social' and 'secret' don't work together".

B. Perceived Risk

Privacy risk beliefs are defined as the expectation of the potential for loss due to the disclosure of personal information online [29]. The risk associated with information disclosure is believed to be a key consideration associated with attitudes towards online information disclosure behavior [30]. An individual's perceived risk is a function of the expected outcomes of information disclosure [31]. The greater the risk a user perceives, the less information they are likely to disclose online. In their privacy calculus model, Dinev and Hart [32] assert that higher perceived risk results in a lower level of trust.

Risk propensity refers to the chance that users will take online in the knowledge of the possibility of a privacy breach against their personal information. Persons with a high level of risk propensity are more willing to knowingly engage in risky behavior. If a service provider is perceived as being honest and reliable in its dealings with a user's personal information, users will perceive little risk in disclosing personal information online [15]. Rather than disclose personal information online based on informed consent, user's sometimes make tradeoffs to minimize perceived risk even though they may feel they have little or no control over these trade-offs [33]. The "value exchange" concept refers to a user's belief whereby they feel they have to disclose personal information online in order to receive the full benefit of interacting online [34]. These apparent trade-offs may also lead to the risky behavior of a "privacy paradox" situation whereby users voice their concerns about revealing personal information online, however they then proceed to unreservedly disclose this information [35].

Research Method

An on-line survey comprising 24 questions, some of which were self-developed questions and others of which were adapted from survey instruments previously published in the literature, was administered to a sample of internet users based in Ireland. 260 usable responses were received.

The questionnaire items captured data about: (1) general demographic variables; (2) attitudes towards online privacy; and (3) perceived online risks, safeguards and controls. Convenience sampling (using a sample that is taken from the population that is easily obtained) was used as the sampling technique. Participants were solicited through personal messages sent via LinkedIn, Twitter, and Facebook. As our population of interest was not the general public as a whole but rather those who have some level of awareness of online privacy issues, the use of social media to attract respondents and the use of a Web-based instrument to collect data are methodologically justifiable. Although it may have been better if the sample was randomized, for practical reasons it was not possible to do so. Nevertheless, we have confidence that the 260 persons who responded provide us with a strong indication of opinion amongst our population of interest because of the high number of responses received and the demographic spread.

Demographics of respondents included the age ranging from 17 to 61, with a mean of 29 years. 60% of respondents were females, 73% of respondents were employed and 82% of respondents were of Irish nationality. The survey data was analyzed in the statistical software package SPSS running descriptive statistics tests, Cronbach's Alpha estimate of reliability test (over .5 is viewed as a reliable estimate) and non-parametric tests of correlation (Spearman's rho, hereafter abbreviated as rs).

We use a 95% level of confidence meaning the value of α (alpha) is 5% (1-.95=.05). Therefore, if our p-value is less than our equal to α, the result is statistically significant. Our correlation tests ran as part of the results section below claim significance as the p-value returned for each test was less than α. The questions that were analyzed as part of this results section are set out in the following tables, including details of their mean, standard deviation and number of responses received.

III. Initial Results

As this exploratory survey is a stepping-stone for further research, the following section presents our preliminary analysis of the data collected.

A. Perceived Control

Analysis was undertaken on the survey questions shown in Tables I to III. Descriptive tests were run, which revealed that 40% of respondents feel they have little or no control over who can view their online information while 66% of respondents indicated that they feel uncomfortable about their personal data being in the control of others. In relation to users' perceived ability to exert control over how their online personal information is used, 84% believe they have little or no control over the actions of other users while 60% of respondents feel that they have little or no control to correct inaccurate or untruthful information about themselves. An overwhelming 81% of respondents feel they have little or no control over "their ability to prevent their data and actions from being used or analyzed by online companies in ways they did not intend". 72% of respondents would be bothered if third parties were to

maintain a history of their online activities and movements, and in this regard it was found that females were found to be more concerned than males.

TABLE I. PERCEIVED CONTROL SURVEY QUESTIONS

How much control do you believe you have over the following issues online (e.g., through policies, privacy settings, etc.): Likert Scale (1= no control at all, 7= complete control)	**Responses (n)**	**Mean**	**St. Dev.**	**Cronbach's α**
Your ability to control who can view your information	240	3.77	1.294	.829
Your ability to control the actions of other online users	241	2.22	1.229	
Your ability to correct inaccurate or untruthful information about yourself	241	3.15	1.298	
Your ability to remove embarrassing or damaging information about yourself	240	3.15	1.281	
Your ability to prevent your data and actions from being used/analysed by online companies in ways that you did not intend	240	2.47	1.230	
Your ability to prevent your data and actions from being used/analysed by other parties in ways that you did not intend	238	2.44	1.267	

Non-parametric correlation tests were also run and it was found that the less control a person perceives themselves as having over their privacy online, the more uncomfortable they feel about information being in the hands of others (rs = -.162). The more control users have over their privacy online, the less likely that their information will be made available to others without their knowledge (rs = -.174). As expected, those who feel they have the least control are also the most concerned that other internet users might abuse their personal information (rs = -.167) and that online companies might divulge their information to other parties without explicit consent (rs = -.178).

TABLE II. TRUST SURVEY QUESTIONS

(Information shared you may want forgotten include personal details such as login details, address, phone number, PPS Number etc.) **How concerned are you that:** Likert Scale (1= not at all concerned, 5= extremely concerned)	**Responses (n)**	**Mean**	**St. Dev.**	**Cronbach's α**
Information you share with Friends may be inappropriately disclosed by them to others	247	2.58	1.210	.881
People you only know online are not who they say they are	247	2.43	1.273	
Other internet users might try to trick or defraud you	246	2.91	1.237	
Other internet users might abuse your personal information	246	3.13	1.187	
Online companies might divulge your information to other parties without your explicit consent	246	3.61	1.086	
Online companies might use your information for purposes other than explicitly stated in their privacy policy	247	3.51	1.104	

TABLE III. PRIVACY DISPOSITION SURVEY QUESTIONS

Please indicate your level of agreement with the following statements: Likert Scale (1= strongly disagree, 7= strongly agree)	**Responses (n)**	**Mean**	**St. Dev.**	**Cronbach's α**
I am generally a private person in my normal everyday life	248	5.56	1.236	.765
I tend to reveal minimal personal information about myself online because I value my rights to privacy	248	5.66	1.281	
I feel uncomfortable about my personal information being in the hands of others	247	5.73	1.320	
I believe there is no need to be concerned about disclosing personal information online	248	2.03	1.304	
It does not bother me that a history of my activities and movements are held by 3rd parties online	248	2.23	1.559	

The level of an individual's perceived control over privacy is also correlated with the amount of information they choose to disclose. The more information they reveal, the less control they feel they have over their ability to prevent their data from being used by online companies in unintended ways (rs = -.137). This is interesting because it suggests that people are giving away their information in the knowledge that they are sacrificing control. It may be that they are happy to do so in the expectation of receiving enhanced online services on the basis of "value exchange" [32] in which they feel compelled to do so in order to avail of fairly normal functionality, i.e. a trade-off. In relation to a user's perceived level of control and the

incidence of adverse experiences, the more control that respondents feel they have over their online privacy, the less often they have ever been the victim of online fraud (rs = -.136) or had an unpleasant experience as a result of online disclosure (rs = -.154). This finding might be interpreted in two ways; it may be the case that some persons feel they are in control because they have not yet had a bad experience, or they may indeed be in control as a consequence of which they have not suffered a breach. However, our respondents overall, feel they have little control over their information once it is disclosed online.

B. Perceived Risk

Analysis was undertaken on survey questions shown in Tables IV and V. Descriptive tests were run which show that the amount of personal information that is revealed online is an important consideration in relation to a person's information privacy. 32% of respondents disclose nothing or only a small amount of personal information, with a further 58% stating they disclose "only what I have to". 74% of respondents either agreed or strongly agreed with the statement "I tend to reveal minimal personal information about myself online because I value my rights to privacy" as to why they withhold information. Those in the age category 33+ are considerably less bothered about potential damage arising from their information being "Accessed by someone you don't want (e.g., employer)" or "Used against you by someone (e.g., to cause embarrassment or spy on you)". This may be because they tend not to disclose as much information online as younger age groups. 50% of respondents believe that something unpleasant might happen to them due to their presence on the internet.

As regards adverse online incidents, 39% had been subjected to privacy violations of some kind, while 20% indicated that their personal reputation was damaged as a result of material posted online. 50% of respondents feel they are not at all protected against damages to their reputation caused by online companies as a result of information disclosed. It is increasingly the case that employers are looking at the online profiles of prospective employees. Therefore, if users partake in risky behavior and it is revealed online, there is the possibility this will affect an aspect of their life for example a relationship or their career. Respondents in this study were in favor of the view that persons should not always be judged on the basis of past behavior (68%). Interestingly 25% of respondents believe it depends how long ago the material was posted online, that users should be held accountable for their actions for a certain amount of time.

TABLE IV. ADVERSE EXPERIENCES SURVEY QUESTIONS

How often have the following events happened to you online? Likert Scale (1= never, 5= all the time)	**Responses (n)**	**Mean**	**St. Dev.**	**Cronbach's α**
Your account was maliciously accessed by an unauthorized person	247	1.45	.666	.657
The privacy of your personal information was violated	245	1.53	.739	
Your reputation was damaged as a result of information posted on online	246	1.24	.545	
You were the victim of an on-line fraud, either on a SNS or elsewhere	244	1.18	.472	
You had an unpleasant experience as a result of information disclosed by you online	246	1.37	.661	

TABLE V. PERCEIVED RISK SURVEY QUESTIONS

Please indicate your level of agreement with the following statements: Likert Scale (1= strongly disagree, 7= strongly agree)	**Responses (n)**	**Mean**	**St. Dev.**	**Cronbach's α**
Overall, I see no real threat to my privacy due to my presence on the internet	240	2.85	1.431	.502
I fear that something unpleasant might happen to me due to my presence on internet	241	4.13	1.431	
I feel safe publishing my personal information online	240	2.9	1.309	
Overall, I find it risky to publish my personal information online	239	4.98	1.429	
It is unlikely that somebody could succeed in gaining unauthorized access to my personal information online	239	2.93	1.527	
Used for commercial purposes (e.g., market research, advertising)	242	3.29	1.441	.845
Made available to unknown individuals or organizations without your knowledge	242	4.05	1.515	
Accessed by someone you don't want (e.g., parents, teacher, employer, ex-friend)	242	4.14	1.564	
Used against you by someone (e.g., to cause embarrassment or spy on you)	241	4.21	1.541	

Non-parametric correlation tests (Spearman's rho) were run and it was found that users perceive it risky to disclose information online as they feel uncomfortable about their personal information being in the hands of others (rs = .457) which reflects possessing a low level of trust. The more often online information is used for commercial purposes; the greater the risk their online accounts will be maliciously accessed by an unauthorized person thus users possess a greater level of trust in people they know than in online companies. A person's privacy online is subject to greater threat due to the risk of

other internet users abusing their personal information (rs = -.312). The more information that is disclosed online by a user, the greater the chance that the privacy of their online information will be violated (rs = -.194). Therefore, overall our respondents believe there is a significant risk to the privacy of their information once it is disclosed online.

IV. Conclusion & Future Research

This study has demonstrated that our respondent's privacy concerns of perceived control and perceived risk determines how much information they reveal. In general they do not feel in control over the information they disclose online and they possess a greater level of trust in people they know online rather than online companies. The majority of respondents stated they only disclosed information online that they were required to; however, some respondents were still subject to privacy violations and reputation damage. Respondents also feel they are at risk due to their online presence and disclosing their information online. Subsequent work will involve further research methods (e.g., focus groups, experiments) to investigate areas of future research arising from the findings of this initial study, including:

1) Why do users feel they have little control over their online information? Are control mechanisms in place and users are not aware of them?

2) Explore the correlation between "value exchange" and users willingness to disclose information online for example why do users feel they have to disclose a significant amount of personal information in order to partake online? Do they actually have to reveal a large amount of personal information in order to gain the full benefits of online interaction?

3) Analyze a trade-off situation involving cost-benefit analysis in which respondents are given an incentive e.g., monetary, to disclose personal information; would the users still only disclose information that they are required to?

4) Conduct a comparison between users living in Ireland with other nationalities to explore if culture has an affect when disclosing information online.

5) Examine the practices that particular websites have in place in relation to information privacy and ask users what these websites could do to improve the confidence they have in these websites.

After further research, findings will provide a greater understanding and awareness of how perceived control and perceived risk affect information privacy online.

References

[1] C.D. Lanier and A. Saini, "Understanding consumer privacy: A review and future directions." Academy of Marketing Science Review vol. 12, no. 2, pp. 1-48, 2008

[2] H.Greenfield, Major study sheds light on online privacy, security values, behavior. Available: http://www.ccianet.org/blog/2013/12/major-study-sheds-light-online-privacy-security-values-behavior/ (Accessed 14 February 2014)

[3] A. Weckler, Almost 70pc Irish people claim data privacy breaches, Irish Independent, Available: http://www.independent.ie/business/almost-70pc-irish-people-claim-data-privacy-breaches-29954042.html (Accessed 14 February 2014)

[4] D. Hardawar, Apple blames bugs for iPhone tracking scandal, software fix coming soon, MobileBeat, Available: http://venturebeat.com/2011/04/27/apple-location-response/ (Accessed 14 February 2014)

[5] A. Moses, PlayStation hacking scandal: police chief says contact your bank now, The Sydney Morning Herald, April 27, 2011. http://tinyurl.com/3wk47eq (Accessed 14 February 2014)

[6] E. Edwards, Protection of data a matter of basic rights, Irish Times, November 16, 2013, Available: http://www.irishtimes.com/news/ireland/irish-news/protection-of-data-a-matter-of-basic-rights-1.1597648 (Accessed 14 February 2014)

[7] F. Bélanger and R.E. Crossler, "Privacy in the digital age: a review of information privacy research in information systems," MIS Quart., vol. 35, no. 4, pp. 1017-1042, 2011.

[8] J. H. Smith, T. Dinev, X. Heng, "Information privacy research: an interdisciplinary review." MIS quarterly vol. 35, no. 4 pp.989-1016, 2011

[9] A. Acquisti and R. Gross. "Imagined communities: Awareness, information sharing, and privacy on the Facebook". In Privacy enhancing technologies, Springer Berlin Heidelberg, pp. 36-58, 2006

[10] T. Dinev and P. Hart "PRIVACY CONCERNS AND INTERNET USE--A MODEL OF TRADE-OFF FACTORS". In Academy of Management Proceedings, Vol. 2003, No. 1, pp. D1-D6, 2003

[11] [N. F. Veltri, H. Krasnova and W. Elgarah. "Online disclosure and privacy concerns: a study of Moroccan and American Facebook users". AMCIS Proceedings, 2011

[12] C. M. Hoadley, H. Xu, J. J. Lee and M. B. Rosson. "Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry". Electronic commerce research and applications, vol. 9, no. 1, pp. 50-60, 2010

[13] M. J. Culnan and P.K. Armstrong. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation".Organization science, vol. 10 no.1, pp.104-115, 1999

[14] T. Dinev, H. Xu, J. H. Smith and P. Hart. "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts." European Journal of Information Systems, vol. 22, no. 3, pp. 295-316, 2013

[15] H. Krasnova, S. Spiekermann, K. Koroleva and T. Hildebrand. "Online social networks: why we disclose." Journal of Information Technology, vol. 25, no. 2, pp, 109-125, 2010

[16] T. Dinev, P. & Hart. "Internet privacy concerns and social awareness as determinants of intention to transact" International Journal of Electronic Commerce, vol.10 no.2, pp, 7-29, 2006

[17] N. K. Malhotra, 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, no. 4, pp. 336-355, 2004

[18] P.A. Norberg, D. R. Horne and A. D. Horne. "The privacy paradox: Personal information disclosure intentions versus behaviors". Journal of Consumer Affairs, vol. 41 no. 1, pp. 100-126, 2007

[19] S.T. Margulis, "Conceptions of privacy: Current status and next steps." Journal of Social Issues vol. 33, no. 3, pp.5-21, 1977

[20] C.A. Johnson, "PRIVACY AS PERSONAL CONTROL" In EDRA; Proceedings of the Annual Environmental Design Research Association Conference, pp. 83, 1974

[21] E.J. Langer, "The illusion of control", Journal of personality and social psychology, vol. 32, no. 2, pp. 311, 1975

[22] R. S. Laufer and M. Wolfe. "Privacy as a concept and a social issue: A multidimensional developmental theory". Journal of Social Issues, vol. 33 no.3, 22-42, 1977

[23] S. T. Margulis "On the status and contribution of Westin's and Altman's theories of privacy". Journal of Social Issues, vol. 59 no. 2, pp. 411-429, 2003

[24] H. Xu, "The Effects of Self-Construal and Perceived Control on Privacy Concerns." In ICIS, p. 125, 2007

[25] S. Grabner-Kräuter, and E. A. Kaluscha, "Empirical research in on-line trust: a review and critical assessment." International Journal of Human-Computer Studies, vol. 58, no. 6, pp.783-812, 2003

[26] D.L. Hoffman, T. P. Novak and M. Peralta, "Building consumer trust online." Communications of the ACM, vol. 42, no. 4, pp. 80-85, 1999

[27] J. Turow, "Americans & online privacy: The system is broken", Annenberg Public Policy Center, University of Pennsylvania, 2003

[28] E. Netchitailova, "Facebook as a Surveillance Tool: From the Perspective of the User." TripleC (Cognition, Communication, Co-Operation): Open Access Journal for a Global Sustainable Information Society, vol. 10 no. 2 p. 687, 2012

[29] C. Posey, P. B. Lowry, T. L. Roberts, and T. S. Ellis, "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, 2010

[30] C. J. Zimmer, R.E. Arsal, M. Al-Marzouq and V. Grover, "Investigating online information disclosure: Effects of information relevance, trust and risk." Information & management, vol, 47, no. 2, pp. 115-123, 2010

[31] T. Dinev, H. Xu, J. H. Smith and P. Hart. "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts." European Journal of Information Systems, vol. 22, no. 3, pp. 295-316, 2013

[32] Dinev, Tamara, and Paul Hart. "An extended privacy calculus model for e-commerce transactions." Information Systems Research, vol. 17, no. 1, pp. 61-80, 2006

[33] J. Rauhofer, "Privacy is dead, get over it! Information privacy and the dream of a risk-free society." Information & Communications Technology Law, vol. 17, no. 3 pp. 185-197, 2008

[34] R. H. Weber, "The Right to Be Forgotten: More Than a Pandora's Box?," Journal of Intellectual Property, Information Technology and E-Commerce Law, vol. 2, pp. 120-130, 2011

[35] P.A .Norberg and D. R. Horne, "Privacy attitudes and privacy -related behavior." Psychology & Marketing, vol. 24, no. 10, pp. 829-847, 2007