CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	The dark side of risk homeostasis when joining a Health Social Network
Authors	Rowan, Wendy;O'Connor, Yvonne;Heavin, Ciara;Lynch, Laura
Publication date	2018-06-01
Original Citation	Rowan, W., O'Connor, Y., Lynch, L. and Heavin, C. (2018) 'The Dark Side of Risk Homeostasis when joining a Health Social Network, ECIS 2018: Twenty-Sixth European Conference on Information Systems, Portsmouth, UK, 23-28 June.
Type of publication	Article (peer-reviewed)
Link to publisher's version	http://ecis2018.eu/published-ecis-2018-papers/
Rights	© 2018 the authors.
Download date	2026-11-04 10:05:32
Item downloaded from	https://hdl.handle.net/10468/7301



UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

THE DARK SIDE OF RISK HOMEOSTASIS WHEN JOINING HEALTH SOCIAL NETWORKS

Research in Progress

Rowan, W. Health Information Systems Research Centre, Business Information Systems, University College Cork, Cork, Ireland, wendy.rowan@ucc.ie

O'Connor, Y. Health Information Systems Research Centre, Business Information Systems, University College Cork, Cork, Ireland, y.oconnor@ucc.ie

Lynch, L. Health Information Systems Research Centre, Business Information Systems, University College Cork, Cork, Ireland, Laura.Lynch@ucc.ie

Heavin, C. Health Information Systems Research Centre, Business Information Systems, University College Cork, Cork, Ireland, C.Heavin@ucc.ie

Abstract

Social networking sites capture, store, analyse and exploit personal data resulting in heightened uncertainty and perceived risk around protecting our personal data. When this data involves personal health information (PHI) the risk factors increase. These risks can be discovered in both the design and presentation of Health Social Networking (HSN) services, as well as the actions of users when providing electronic consent (eConsent). How do users interact with technology and determine the potential risks to their PHI data? This paper seeks to explore users' behaviours and reflections on risk taking when registering onto a HSN. Examining users' registration behaviours, it is possible to explore users' risk homeostasis when providing eConsent on a HSN. This paper focuses on understanding the users' decision making process to the reading and comprehension of the Terms and Conditions (T&Cs), and Privacy Policy (PP) statements. A two-step approach was taken to collecting data, with 1) the observation of action followed by 2) a focus group discussion. This research sheds light into user's assessment of future risk, the potentially dark side of sharing PHI and the preferred ways of operating for the user of these online communities.

Keywords: Risk; Decision Making; eConsent; Health Social Networks (HSNs).

1 Introduction

"*The updated version of Descartes's Cogito is 'I am seen, therefore I am' – and that the more people who see me, the more I am…*" (Bauman & Donskis, 2013)

Information overload has become part of the information revolution, providing end users with a greater range and minutiae of knowledge (Sundar, Knobloch-Westerwick, & Hastall, 2007). Latterly, information overload has been combated by the use of visualisation, aiming at reducing human effort and increasing human attention by improving the user's information processing capacities (Chung, Chen, & Nunamaker Jr, 2005; Pirolli, Card, & Van Der Wege, 2001). Contrary to this, the presentation of informed consent on electronic platforms (referred herein as eConsent) has remained woefully underdeveloped, remaining overly text heavy. The users of Health Social Network (HSN) platforms are faced with Terms & Condition (T&Cs) and Privacy Policies (PP) statements that are at least four pages long, with heavy technical jargon. This paper aims to explore users' behaviours when providing electronic consent (eConsent) on a HSN. More specifically, the focus is on user engagement and judgement of risk for their Personal Health Information (or lack thereof) based on their interaction with the T&Cs and PP statements on the HSN.

HSNs enable patients/users to share health experiences that can improve their lives – especially those diagnosed with chronic diseases (O'Connor & Heavin, 2016). HSNs are a service where users can find health resources i.e. emotional support and information sharing with peers, as well as Q&A's with Physicians. These services are primarily directed at patients to build peer affinities and experience collective learning (Swan, 2009). However, prior to using a HSN, users are required to provide consent as part of the site registration process. The concept of informed consent was brought into medicine through courts and government agencies (Beauchamp, 2011). The purpose of informed consent is to ensure that enough of the correct information is provided to the individual to make them aware of the potential risks and benefits associated with participating in a specific research study or in using a specific service, and in so doing protecting and assisting them in meaningful choice (McGuire & Beskow, 2010). Users often share vast amounts of Personal Health Information (PHI) on HSNs as part of their engagement with the community however, in some cases users are not familiar with the HSNs privacy policy to know whether their PHI is safe (O'Connor & Heavin, 2016).

1.1 Contextual Matters

On a HSN platform the eConsent process is presented to users as an adhesion contract, offering their services on a "take it or leave it" basis – simply ticking agree to continue (Bashir, Hayes, Lambert, & Kesan, 2015). However, this does not fully meet some of the requirements of informed consent as proposed by Faden & Beauchamp (Faden & Beauchamp, 1986) in which comprehension and voluntariness are important factors. User comprehension is negated when individuals do not read and understand the T&Cs and PP statements of the site they are signing up to (Obar & Oeldorf-Hirsch, 2016) and voluntariness is impeded by the "take or leave it" approach to eConsent offered by the HSN (Bashir, et al., 2015). It is important to note that a HSN registered in a specific jurisdiction is governed by that country's data protection laws e.g. in USA, the Health Insurance Portability and Accountability Act (HIPPA 1996) regulates private health information (PHI). With the new General Data Protection Regulations (2018) due to become law in May 2018 there will be a strong emphasis on the transparency, security and accountability of online data use (GDPR, 2017). Yet, questions remain as to whether the GDPR (2018) will have data protection jurisdiction over USA based services.

1.2 Individual Matters

It can be said that HSN user interfaces are not the only problem when it comes to security and privacy risks – user's level of interaction with technology and their decision making are effected by their emotional and cognitive estimation of risk (West, 2008). Much research in the social sciences sug-

gest that individuals are often less than optimal decision makers when it comes to judging risk (Adams & Sasse, 1999; Slovic, Fischhoff, & Lichtenstein, 1986). For instance, in situations of uncertainty in decision making, it was found (Valérie Burri, 2009) that individuals with a limited knowledge base would use analogies and personal experiences as tools for reasoning, and choice selection. There is also evidence that a 'privacy paradox' can exist – where there is a discrepancy between user's concerns about privacy and their actual online behaviour to protect their privacy (Sundar, Kang, Wu, Go, & Zhang, 2013). Additional research (Sundar, et al., 2013) found that many online users' privacy disclosure behaviours were driven by heuristics (mental shortcuts) rather than by estimates of risk versus benefit. The use of mental shortcuts has long been realised in social cognition – the human as a "cognitive miser" making decisions based on quick and cursory reasoning, negating the need for effortful thinking (Morris, Woo, & Singh, 2005). The cognitive miser approach allows individuals to simplify complex problems and emphasize efficiency (Kim & Mrotek, 2016). Yet, motivation and emotion also play a role in decision making which has led to the view of the person as not just cognitive actors but as motivated tacticians – using cognitive strategies based on goals, motives and needs. Sometimes these tacticians choose accurately and adaptively, and on other occasions they choose in the interest of self-esteem or speed (Fiske & Taylor, 1991).

Often individuals do not believe they are vulnerable to risks online (West, 2008). Some individuals maintain an acceptable degree of risk that is self-levelling, i.e. risk homeostasis (Wilde, 2001). For instance, users who increase their security measures would then be more likely to increase their risk behaviours. There are a number of factors that could influence these risk taking behaviours – a lack of motivation, the concept of safety being too abstract in the online setting, a lack of immediate feedback (delay in consequences), and the amount of user effort involved in evaluating the security/cost trade off (West, 2008). There is also evidence in the literature that a range of motives for individual risk taking exist including them seeking a sense of power, control, thrill, challenge, escape, or fulfilment of other needs (Powell, 2007). Individual's view of risk may be influenced by psychological, social, cultural or institutional considerations (Finucane, Alhakami, Slovic, & Johnson, 2000). Research (Renn, 1998) states that the perception of risk can be affected by intuitive biases such as the significance of the information to the person, the events experienced and whether this experience either supports or refutes prior experience – in the latter case, there would be an avoidance of cognitive dissonance (a disparity between one's belief system and a presenting situation). The view of risk may become downplayed or ignored to avoid the internal tension that cognitive dissonance could create (Renn, 1998). In Risk Homeostasis theory everyone is considered to have the ability to take a risk, but this varies between individuals (see the work of Slovic, 2016). Risk assessment is conducted by individuals via an evaluation of outcomes, based on our own experiences or our knowledge on the experiences of others (J. Adams, 1995). Four factors have been identified as determining the level of risk:

1. The expected benefits of risk behaviours e.g. saving time by ignoring safety measures.
2. The expected costs of risk behaviours e.g. time and effort to recover from a computer threat.
3. The expected benefits of cautious behaviours e.g. maintaining confidentiality and integrity of information.
4. The expected costs of cautious behaviours e.g. effort in engaging with complicated security procedures (Powell, 2007).

In attempts to induce individuals to reduce their risk taking behaviours, proposals have been made focusing on three strategies – 1) persuasion of individuals to change behaviours; 2) the introduction of law to impose behavioural change and 3) to provide automatic protection in the product or in environmental design (Hedlund, 2000). Other human factors can inhibit the reduction of risk, including the optimism bias where individuals believe the level of risk is lower for them than other individuals, and the normalization of risk, where individuals learn to accept risk based on a desensitization process from prior experiences (Celsi, Rose, & Leigh, 1993). It is posited (Kearney, Kearney, Kruger, & Kruger, 2016) that the concept of risk homeostasis provides rich insights into contradictory human behaviour. With Information Technology (IT) there is an application of the risk homeostasis theory to users when they engage in the knowing-doing gap or the Privacy Paradox - the discrepancy between users concerns about privacy and their actual online behaviour to protect privacy (O'Connor & Heav-

in, 2016). A self-levelling risk adopted by users, attempts to prevent the cognitive strain involved in decision making, whether under time constraints or overloaded with information e.g. reading lengthy T&Cs and PP statements. With these arguments in mind, this research seeks to explore the users' perspective, by asking how and why they took the action to provide eConsent on a HSN, and on what basis did they estimate the potential risks for their PHI. The following sections of this paper will detail the research design, the findings and the conclusions exploring the bright or dark side of joining an online community.

2 Research Design

This ongoing research funded by the Wellcome Trust is in the final phases of a 12-month project. Ethical approval was provided by the Social Research Ethics Committee, University College Cork, Ireland.

An experimental, qualitative approach was taken to the collection of data, with the observation of registration behaviours followed by focus group discussions. This approach was adopted as it offered the potential to explore the "how" and "why" questions as a means of exploring the nuances of users' perspectives when registering to a HSN. A similar approach was employed by Sutanto, Palme, Tan & Phang (2013) when exploring the personalization-privacy paradox of smartphone users. Research (Miles & Huberman, 1994) suggest qualitative studies allows one to capture the "others" perception of an experience. A bottom up – thematic approach was taken to the analysis of focus group data. Thematic analysis (TA) offers a method for identifying and analysing patterns in qualitative data. TA has theoretical flexibility as it can be applied within a range of theoretical frameworks, from essentialist to constructionist. It is also suited to a range of research interests, research questions and research data (Clarke & Braun, 2013). NVivo provided the qualitative analysis package for the transcripts of data collected from focus group discussions. The data was thematically grouped into pertinent topics identified from the participants' contributions.

In Step 1 participants were asked to register onto a HSN using mock registration details supplied by the research team. Whilst participants undertook this activity, researchers observed their behaviours while the participants used mobile devices to register on the HSN. The experimenter effect - Hawthorne (Adair, 1984) - was considered, but due to the nature of the research, observation was considered a vital part of the design process.

Step 2 participants were then asked to take part in focus group discussions. These were audio recorded and later transcribed. A total of three focus groups were held. Participant numbers in each focus group were 10:8:6 respectively.

2.1 Sample

Twenty-four participants took part in this research. The gender ratio was Male 3:1 Female. Ages ranged from 18 to 44 years, with the majority of participants were in the 25-34 age bracket. There is the continuing problem in research in using a laboratory setting for the administration and collection of data, but Briggs et al (1996) suggests that graduate business students can provide a surrogate for "real world" users. In this study, participants were graduate students from University College Cork, Ireland.

2.2 Coding of Responses

The focus groups were labelled as FG1, FG2 and FG3 respectively. Participants within these focus groups have been anonymised by using Gender/Number coding e.g. M1, M2 or F1, F2. When a group response or consensus agreement was made within discussions this is coded as FG1 (Focus Group 1): GR, the later abbreviation representing "general response".

3 Results

The observation of participant behaviours during registration onto a HSN revealed that very little time was taken to complete the three pages of this process. When participants were asked to provide eConsent at the bottom of the first page on registration, less than 1 minute was taken by participants to make the choice to click – agree. For participants to read and understand the T&Cs and PP statements it would involve clicking a link, redirecting users to different pages on this website. It is quite clear from these observations that participants were not information seeking, were not moving onto different pages with these details, but simply ticking "agree". It was apparent that participants were not taking into consideration, at any deep level, the potentially negative implications or benefits of their decision to join this HSN.

3.1 Just Click

Comments made by focus group participants revealed that 'Just Clicking' agree was automatic or embedded into their repertoire of behaviours when interacting with computer interfaces requesting consent. Table 1. details the reflective comments made by participants when discussing their 'just click' behaviours.

Participant ID	Just Click Comments
FG3:M5	"I always just tick that and never look at it."
FG3:M2	"So, used to ticking it at the bottom, so I just tick the box."
FG1:F1	"You want to use the app, you are going to use it regardless of the terms and conditions."
FG1:M1	"You are going to agree, even if you are not sure about that point, or not sure about this point, I think you are still going to go ahead and tick agree.
FG3:F1	"I always agree" … "if you don't click it, then you get nothing."
FG1:F3	"…you either agree and use it, or don't agree, and not use it. There's no room for negotiation..."
FG2:M2	"(Ticking Agree) …Yes, it's a habit."

Table 1. The Just Click Agree Habit.

The unconscious and automatic habit of ticking agree to this HSN could be said to be a form of conditioned learning. Past experiences of engaging with websites had taught users that this step had to be completed to gain access, that the conditions offered were non-negotiable. Although users may have had or still had concerns over eConsent the decision risk had become normalised, which were evidenced in the self-levelling actions.

3.2 Sharing Risks

Through discussions on the T&Cs and PP of this website, it became more apparent that participants were less comfortable about the potential risks for their personal health information (PHI). A reflective dissatisfaction emerged on how their PHI data could be used because of joining a HSN. Concerns were expressed about who users were sharing their information with i.e. other members as strangers; The potential for their PHI to be leaked or hacked; Employers or insurance companies being able to discriminate against users based on the health information they supplied to HSNs and; the general safety and confidentiality of their PHI on the HSN. Table 2 provides comments from participants on these issues. The irony being that had participants read the T&Cs and PP statements prior to giving eConsent they could have made a more informed choice about joining, and following this perhaps not felt "regret" at the decision taken.

Participant ID	Risk Reflections
FG1:F2	"I think you are lulled into a false sense of security … I mean you wouldn't discuss your health issues in a doctor's waiting room, but you are more than happy to put it in here for a community."
FG1:M3	"There is a lot of wrong information, misinformation out there, … you know health improvements or thing that improve your health, really they are giving us anecdotal evidence, there is no real hard clinical evidence for it."
FG1:M4	"In the T&Cs they were absolving themselves from any obligation for false information, … if you don't read it, … you might just think "oh well this person is going through the same thing so, it worked for them, so just do what they did."
FG1:M3	"You'd want some control over data, otherwise employers might discriminate, or health insurances definitely will."
FG1:M5	"Assurances were given about confidentiality … but in the real world I would be very guarded. I would be a bit concerned about traceability."
FG1:M3	"There's no-one that can guarantee that your data is safe, so it does not matter what they promise you."
FG1:M4	"The biggest challenge for the 21st Century is personal, how to save your personal data."

Table 2. The potential darker risks of sharing PHI data on HSNs.

Other topics yielded from further discussion highlighted IT literacy and comfortability discrepancies among participants. Some participants were more IT confident than others, and had a deeper understanding on how personal information could be used and interconnected with other websites / applications. Participant comments illustrated in Table 3 display views on the realities of inputting PHI online, the sharing implications and how links to other website providers could be used as secondary data sources by other unknown third parties. Users with this type of internet knowledge were in a better situation to manage any perceived security threat (Büchi, Just, & Latzer, 2017; Lee, Tan, & Siah, 2017).

Participant ID	Security and Connectivity
FG1:M4	"There wasn't much reference made to inform the user, … it was all hidden inside a legal document."
FG2:M5	"It's enough to have a piece of information that is correct … to find everything about you." "Social, health profile is one component of your profile that big companies are using." "If I pay Google enough they can sell me your personality. Your profile, even more information than you know about you."
FG2:M6	"Joining the dots basically."
FG1:M5	"Even down to what you are buying, eating, everything is integrated."
FG2:F1	To control Connectivity: "I don't want the intersection. I would not put a health app on my phone because I don't want the other apps getting access to data to do with health. So, I look at where they are going to intersect and separate them that way."

Table 3. The potential dark risks for the secondary use of PHI data on HSNs.

3.3 User Protection

The next steps suggested by participants involved providing assurances to users of HSNs, these included recommendations for altering the HSN registration process particularly focusing on changing the provision of eConsent. These included:

- To provide some legal backing to PHI – data protection – and to impose fines on those that do not meet these requirements.
- To offer the user different levels of control over who can access their PHI, and how much of this information they are required to share with others.

- To make the registration and comprehension of eConsent a more user-friendly process, so that both the content and presentation of information is more digestible to a lay audience.

Table 4 presents feedback on the proposed changes for the use of PHI data on HSNs and the potential reduction of risks from the user perspective.

Participant ID	Changes for PHI protection – the user perspective
FG2:F2	"If there was a real legal backing to the protection of information … I'd be more comfortable, but I don't think legally there is." "also, accountability. If this information that you are entering is being used, is going to be used for a purpose, for something it was not intended, who is going to be accountable and what will the consequences be?"
FG2:F1	"To have different levels of access and you can share with people like that."
FG3:M2	"At the very minimum, an opt in to sharing, not automatically opt into it."
FG1:F3	"If there was an on-boarding process to tell you – this is what you are signing up for - … so that you are aware and then it's your choice to complete it or walk away."
FG1:M2	"I think it would be better to see who's viewed your profile, who's viewed what health problems you have."
FG2:M2	"They (the PP and T&Cs) should be legally decoded, and be brief to be absorbed."
FG1:M3	"I think it's much easier if it is simple language, text, saying what they actually intend to do with what you have put onto the social network."

Table 4. Protection options for PHI data on HSNs.

Moving forward, it is apparent that although users are currently exposing their PHI data to little understood levels of risk, when their levels of awareness are raised the user response is quite clear – "to provide us (the user) with the tools, knowledge and ability to control the risk levels that our PHI data could be exposed to".

4 Discussion

The aim of this research was to explore users' behaviours when providing eConsent on a HSN. With the focus on users' engagement and judgement of risk for their PHI (or lack thereof) based on their interaction with the T&Cs and PP statements on the HSN. Findings suggest that a privacy paradox exists for some participants in this group by simply "ticking agree" to eConsent on registration to this HSN. So, are users taking the dark risks of sharing PHI data in online communities seriously? Prior experience has taught users that 'ticking agree' offers access to sites, so whether you agree with the sites T&Cs and PP statements or not, any concerns you might have are easily overridden when the motivation or drive to get access to a service is high. It can be stated that these users were taking dark risks with their PHI data at time of eConsent, but were content with this risk homeostasis. It was only when users reflected on the potential security risks for their PHI data, after registration and upon reflection, that the potential dark risks were consciously considered and dissatisfaction emerged. Research participants then presented a clear picture of their future requirements in service design - they would like to regain control over the access and use of their data by HSN sites (a summary illustration of findings is provided in Appendix A – Figure 1).

The darker side of risk taking in online HSN communities has been illustrated by users in this research. There was a lack of user motivation to read the T&Cs and PP information in their current form. There was also the issue of security risk consequences being too distant from users' comprehension, resulting in the immediate action of "ticking agree". The expenditure of effort required for the end user to fully engage with the current presentation of T&Cs and PP statements (lengthy, text heavy documents) has a detrimental effect on intention behaviours – in other words, discouraging users from information seeking to enable eConsent to be a truly informed choice. Findings from this research are in line with a consumer report that states 'Users do want more control over the collection and use of their data' (Center, September 2008). However, offering users more control in isolation

from other steps (such as education and regulation) would not be a panacea for all ills. To move forward there is a need to increase user awareness on the potential benefits of using cautious behaviours – securing the integrity and confidentiality of their online PHI data.

Every research study has limitations; this also applies here. The sample size of participants that took part in this study could be criticised as being too small or too restrictive to be generalisable. However, given the exploratory nature of this study, the primary objective was to gain insight into user views and perceptions of the HSN eConsent process, and examine the risks for users joining such a community. The use of qualitative methods has provided a greater understanding of "the other" or "the HSN user" views and has provided illuminating findings. Using mock profiles may have distanced users from inquiring about privacy risks for their PHI data, however the rationale for this was to protect participants' privacy whilst taking part in this study.

5 Conclusion

The next steps for this research will delve further into users' needs when providing eConsent on HSN platforms and will focus on assisting the user through the exploration of the design of privacy communication for service users. With new laws on the horizon in the form of the European-wide data protection legislation (GDPR) in 2018, movement is afoot to improve the protection of users' online data. As such the user is centre focus in terms of improving data protection.

This research contributes new insights on how eConsent within HSNs could be designed to increase users' understanding and awareness of the use of their PHI use while minimising the risks the end-users. For developers of mobile applications (e.g. HSNs) who face increasing pressure to address information privacy issues due to the introduction of GDPR, this study provides practical guidance on how the eConsent process could be enhanced. Users should be educated on the potential risks for their shared PHI data and how to minimise these dark risks; there must be a more emphasised focus on the regulation of eConsent by the introduction of legislation; or in the redesign of the eConsent process on HSN platforms, perhaps moving to a dynamic consent process or incorporating a movement to privacy-by-design in the creation of these online communities. The design of eConsent on HSN platforms needs to move forward, by improving the clarity on PHI sharing risks and security issues, informing the end user by making it easier for them to comprehend these potential consequences. This must come in the form of education increasing user awareness and IT literacy, so that decision making on risk taking is on a truly informed consent basis. When users become more informed participants in the eConsent process, it is more likely that a behavioural change will result – users becoming more confident at selecting the sharing levels for their PHI data. A confident user is an informed participant in protecting their online data, reducing any sense of regret on a decision to join and moving the HSN user to the brighter side of online sharing.

From a theoretical perspective, this study highlights that some individuals maintain an acceptable degree of risk that is self-levelling, i.e. risk homeostasis. In exploring this phenomenon, this research extends existing behavioural-based literature by highlighting the need to explore risk homeostasis as a factor or an influential theory in the Information Systems field. Moreover, this study addresses an under-investigated area of research focusing on the electronic consent process. In doing so, this research addresses a broader challenge of how to ensure that citizens are aware and understand how their data/information is stored, processed and used in this digital age.

Acknowledgements

We would like to acknowledge the Wellcome Trust Grant – CHASM Project seed award 201607/Z/16/Z.

References

Adair, J. G. (1984). The Hawthorne effect: A reconsideration of the methodological artifact. *Journal of applied psychology, 69*(2), 334.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Adams, J. (1995). Risk, University College London Press. *London, UK*.

Bashir, M., Hayes, C., Lambert, A. D., & Kesan, J. P. (2015). *Online privacy and informed consent: The dilemma of information asymmetry.* Paper presented at the Proceedings of the 78th ASIS&T Annual Meeting: Information Science with Impact: Research in and for the Community.

Bauman, Z., & Donskis, L. (2013). *Moral blindness: The loss of sensitivity in liquid modernity*: John Wiley & Sons.

Beauchamp, T. L. (2011). Informed consent: its history, meaning, and present challenges. *Cambridge Quarterly of Healthcare Ethics, 20*(4), 515-523.

Briggs, R. O., Balthazard, P. A., & Dennis, A. R. (1996). Graduate business students as surrogates for executives in the evaluation of technology. *Journal of Organizational and End User Computing (JOEUC), 8*(4), 11-19.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: the importance of Internet skills for online privacy protection. *Information, Communication & Society, 20*(8), 1261-1278.

Celsi, R. L., Rose, R. L., & Leigh, T. W. (1993). An exploration of high-risk leisure consumption through skydiving. *Journal of consumer research, 20*(1), 1-23.

Center, C. R. N. R. (September 2008). *http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html* -

Chung, W., Chen, H., & Nunamaker Jr, J. F. (2005). A visual framework for knowledge discovery on the Web: An empirical study of business intelligence exploration. *Journal of Management Information Systems, 21*(4), 57-84.

Faden, R. R., & Beauchamp, T. L. (1986). *A history and theory of informed consent*: Oxford University Press.

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of behavioral decision making, 13*(1), 1.

Fiske, S., & Taylor, S. (1991). McGraw-Hill series in social psychology. *Social cognition. New York: Mcgraw-Hill Book Company*.

GDPR. (2017). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

Hedlund, J. (2000). Risky business: safety regulations, risk compensation, and individual behavior. *Injury prevention, 6*(2), 82-89.

Kearney, W. D., Kearney, W. D., Kruger, H. A., & Kruger, H. A. (2016). Theorising on risk homeostasis in the context of information security behaviour. *Information & Computer Security, 24*(5), 496-513.

Kim, H.-S., & Mrotek, A. (2016). A functional and structural diagnosis of online health communities sustainability: A focus on resource richness and site design features. *Computers in Human Behavior, 63*, 362-372.

Lee, W. Y., Tan, C.-S., & Siah, P. C. (2017). The Role of Online Privacy Concern as a Mediator between Internet Self-Efficacy and Online Technical Protection Privacy Behavior. *Sains Humanika, 9*(3-2).

McGuire, A. L., & Beskow, L. M. (2010). Informed consent in genomics and genetic research. *Annual review of genomics and human genetics, 11*, 361-381.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*: sage.

Morris, J. D., Woo, C., & Singh, A. (2005). Elaboration likelihood model: A missing intrinsic emotional implication. *Journal of Targeting, Measurement and Analysis for Marketing, 14*(1), 79-98.

Obar, J. A., & Oeldorf-Hirsch, A. (2016). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services.

Pirolli, P., Card, S. K., & Van Der Wege, M. M. (2001). *Visual information foraging in a focus+ context visualization.* Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.
Powell, C. (2007). The perception of risk and risk taking behavior: Implications for incident prevention strategies. *Wilderness and Environmental Medicine*, *18*(1), 10-15.
Renn, O. (1998). Three decades of risk research: accomplishments and new challenges. *Journal of risk research*, *1*(1), 49-71.
Slovic, P. (2016). *The perception of risk*: Routledge.
Slovic, P., Fischhoff, B., & Lichtenstein, S. (1986). The psychometric study of risk perception *Risk evaluation and management* (pp. 3-24): Springer.
Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013). *Unlocking the privacy paradox: do cognitive heuristics hold the key?* Paper presented at the CHI'13 Extended Abstracts on Human Factors in Computing Systems.
Sundar, S. S., Knobloch-Westerwick, S., & Hastall, M. R. (2007). News cues: Information scent and cognitive heuristics. *Journal of the Association for Information Science and Technology*, *58*(3), 366-378.
Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *Mis Quarterly*, *37*(4).
Valérie Burri, R. (2009). Coping with uncertainty: Assessing nanotechnologies in a citizen panel in Switzerland. *Public Understanding of Science*, *18*(5), 498-511.
West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34-40.
Wilde, G. (2001). J (2001): Target Risk 2. Second (revised) edition: Toronto, PDE Publications.

Appendix A.

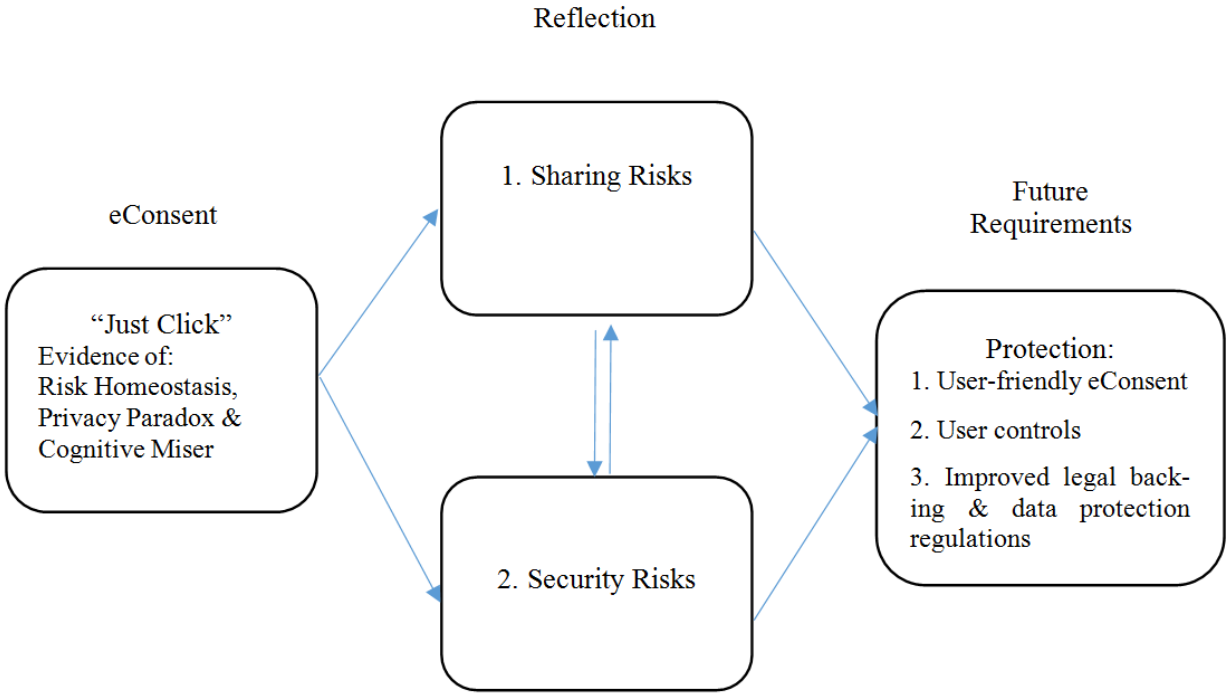


Figure 1. Summary illustration of findings from this study.