12-15-2019

Does privacy mean different things to different people: Can that explain privacy paradox?

Sanjay Goel

Kevin Williams

Jingyi Huang

Alan Dennis

DOES PRIVACY MEAN DIFFERENT THINGS TO DIFFERENT PEOPLE: CAN THAT EXPLAIN PRIVACY PARADOX?

Sanjay Goel, Kevin Williams, Jingyi Huang
University at Albany, State University of New York
Albany, NY 12222

Alan Dennis
Indiana University
Bloomington, IN 47405-7000

ABSTRACT

Privacy is considered a fundamental inalienable right in most western democracies, and yet the understanding of privacy varies considerably among people. Research shows that people exhibit several paradoxical privacy behaviors. We contend that some of these paradoxical behaviors are related to privacy literacy. In this research we define privacy literacy and present scales to measure this literacy. We then associate the paradoxical behaviors with privacy literacy. We also contend that temporal discounting plays a significant role in some paradoxical behaviors because some individuals place a high value on short-term rewards which cause them to behave in ways that may be counter to their long-term intentions. Our overarching research goal is to understand the motives (e.g. tangible rewards, curiosity, fame etc.) that lead users to voluntarily disclose their private information.

Keywords: privacy, security, individual differences, personality, privacy paradox

INDTRODUCTION

In the context of the internet, there has been strong advocacy for user privacy protection and rules for privacy protection (e.g., GDPR) keep getting stronger. GDPR and similar regulations in other countries assume that privacy is important. We also know that individuals routinely claim they value privacy but act in ways that suggest that they don't. That is, *espoused* privacy (what we say) is very different from *enacted* privacy (what we do). While the notion of privacy seems important, is privacy that important to most people in everyday life? There may be long-term benefits of privacy, but there may by immediate gratification from disclosing information that outweighs the need for privacy. One explanation of the privacy paradox lies in the concept of temporal discounting (e.g., Green Fry and Myerson 1994; Rachlin and Raineri 1992), wherein people prefer immediate gratification to long term benefits.

There has been considerable research in understanding the privacy paradox, wherein people voice strong concerns for privacy while doing little to protect their personal data and voluntarily revealing their information in public forums such as social media. Needs for privacy vary in different situational contexts; a person may be very secure about their financial information but very careless about their health information. A person may be willing to have Alexa listen and record conversations in their home, but be opposed to video surveillance on public streets. The privacy calculus will vary among individuals from a situational context, based on individual propensities of risk in different domains.

There are several unanswered questions related to privacy. How do people interpret and understand the concept of privacy, and is there a way to measure this understanding? Also, do people have different desires for privacy across different contexts and/or with different types of information? Finally, how much privacy do users really want, and when do they want it?

There is extensive research on the issue of privacy paradoxes, the privacy calculus, and biases related to privacy decisions, however, the role of dispositional and situational factors in privacy decision analysis has not been comprehensively addressed. We plan to examine the role of personality in privacy calculus and how the privacy calculus morphs based on contextual changes. We plan to take a two-dimensional grid with one dimension being privacy attitudes, and the other being utility from disclosing private information, and map personality factors across the grid. As a precursor to this research, we will attempt to understand how people interpret and understand privacy in different contexts. We present results of this data collection and discuss our overall research design for our future research. The rest of the paper is organized as follows: Section 2 provides a review of the literature; Section 3 provides our data collection and results, and Section 4 provides the design for our overall research, followed by concluding remarks.

LITERATURE

The Privacy Paradox can be defined as a set contradictory attitudes towards privacy. One instance is the concurrent desires to be left alone and to be popular; people strongly feel the need for privacy, however they reveal their information freely on social media to improve their social standing. Another instance is having strong attitudes towards privacy and yet giving it up for minor gains, such as access to a website or a promotion (Acquisti 2004; Barnes 2006). Many users state a positive attitude towards privacy-protection behaviors, but are derelict in their own actual privacy behavior (Joinson et al. 2010; Pötzsch 2009; Tsai et al. 2006). Furthermore, while there may be an intention to limit the disclosure of sensitive data, users often disclose a lot more than they intend (Norberg et al. 2007). Users understand the privacy risks of revealing data online, yet they willingly disclose personal information for small gains like access to information or getting discounts (Acquisti and Grossklags 2005; Sundar et al. 2013). In the same vein, users

disclose personal information on social media for perceived gains, such as popularity or belongingness (Hughes-Roberts 2012; Manier and O'Brien Louch 2010; Nagy and Pecho 2009; Yoo et al. 2012).

There has also been extensive research on privacy calculus, aka decision analysis, when making privacy choices. Decision models can vary from purely heuristic or impulsive to purely analytic. Privacy decisions explained by rational choice theory (Simon 1955) are based on purely rational decision making (Li et al. 2010; Keith et al. 2013; Li 2012; Culnan and Armstrong 1999) whereas heuristic models are based on preprogrammed responses based on past experience (Kahneman, 2011). Most of the models lie in the middle of the two extremes, where biases are incorporated into the user's rational decision making. The variables for rational choice include financial gain, services, status and love, belongingness, convenience, and fame (Donnenwerth and Foa 1974; Foa 1971) whereas disclosure risks include embarrassment, security exposure, profiling, and lack of opportunity or victimization based on profiling. The biases in rational choices can include under/over estimation of risk, temporal discounting (immediate gratification) of gains/losses, optimism etc.

Pentina et al. (2016) studied the role of personality and cross-cultural differences in the privacy calculation model, and found that extraversion and agreeableness decreased the risk perception of privacy decision making in all cross-cultural situations. They also note that satisfaction of informational and social needs led to privacy disclosure. The link between personality and privacy is under-developed; there are many more personality traits that may link personality to privacy behavior, for instance, people high in extraversion or sociability may disclose information more easily and people that rank high in neuroticism may tend to keep information private. Another trait that is likely to be related to divulging personal information is

the need for affiliation (the need to feel a sense of belonging within a social group), which is related to willingness to share. Also, personality traits may predict certain types of privacy behaviors but not others. For instance, Sociability or the need for affiliation might predict willingness to share socially-oriented information (e.g., activities on FB), but will be unrelated to sharing health information. An individual difference like risk perception or trust in might be predictive in both situations Consequently, we need to examine dispositional and situational factors in conjunction. Another important question is the connection of personality to the privacy paradox i.e. to situations when a person's privacy intentions and beliefs don't correspond to their privacy actions. Perhaps people low on the conscientiousness scale or high on the opportunistic scale would show paradoxical behaviors in relation to information disclosure.

DATA COLLECTION AND ANALYSIS

The concept of privacy is often vague for people, and they make their privacy decisions based on different understandings. The goal of this project is to understand how users interpret privacy in general, and across different domains. To understand the interpretation of privacy we designed a survey to ask people about their privacy interpretation and understanding. We surveyed participants with some open-ended questions. In total, we received answers from 34 participants located in the U.S. (14 Males, 17 Females, 3 missing, mean age = 40.43, S.D. = 11.11). We asked participants to define "privacy" in their own words. The definitions provided by the participants were very consistent, almost all of them distinguished between "self" and "others" and mentioned the ability to keep information to the "self" at will. One example of the definitions is "Privacy means that other people don't have information about me unless I specifically give it to them/allow them to have it. It also means that I have a place that is a refuge that people can't see me or know what I am doing."

We further asked participants to define privacy in specific domains, such as workplace, health-related information, financial information, personal relationships, online activities, location/schedule information, and conversation-related information. Regarding privacy in the workplace, there are several different aspects mentioned by participants: 1) non-work-related personal information not disclosed to the organization without permission; 2) the ability to keep personal space without being disrupted; 3) securing the organizational data; 4) personal work related information like habits and style. In domains other than work, people's definitions on privacy are quite consistent. The table below provides some examples of definitions in areas other than workplace information. In addition to the dimensions listed, our participants added several more areas such as children's information, political affiliation, religion, home address and other personal identifying information, personal environment privacy, and the contents of digital devices, the privacy of which they considered important.

We further asked people to sort the privacy domains according to their importance. Participant answers were very different in this case. Some people viewed all domains as equally important (e.g., "I answered the same for most because privacy is very simple and straightforward for me, it is black and white, no grey areas. I have one basic perspective and it is above all else the most important aspect in anyone's life who wishes their life to be told only on their terms."), while others regard some domains as particularly important and others as less so. Financial privacy and personal relationship privacy are the ones most often listed as most important.

Table 1. Privacy domains and examples of participants' definitions to these domains.

Domains	**Examples of definition**
Health-related information	Privacy of health-related information means that doctors, hospitals, and insurance companies must respect the sanctity of people's personal

	medical situations, which may be embarrassing, sensitive, and or potentially harmful financially or socially if discovered. People have a right to visit a medical professional and know that, unless necessary for medical purposes, their details will not be shared with others.
Financial information	Being able to keep my financial information, transactions, dealings available for my eyes only or that of my financial institution. Credit cards, taxes, bank accounts, stocks, bonds, loans, etc. should be available for my eyes only or those that I specifically give permission to.
Personal relationship	1) This means any type of relationship I have with people, or even organizations should not be disseminated, as it [doing so] may bring harm to me or anyone associated with me. 2) You can be in a relationship with someone and no one needs to know what you two are doing except you two. Nobody needs to know if you are having sex, if you plan to have kids, hell, what you had for dinner…nobody needs to know NOTHING without your permission.
Online activities	It either means doing these activities anonymously, or it means understanding how information about my activities will be used, or it can mean limiting what entities can have access to in my history.
Location/schedule information	It means your location is not tracked, and details about your schedule are not made public or shared with anyone other than those you authorize.
Conversation-related information	1) It means that whatever I share with someone by speaking with them must not be shared with anyone else unless I have given my permission to do so. 2) It must be announced that my call to a business is being recorded, and those recordings will only be heard by people trying to improve customer service. Recordings in other contexts should similarly be announced.

All participants considered privacy as either very important or extremely important (rated on a 1-5 scale with 1 as extremely important and 5 as not at all important, mean = 1.48, S.D. = 0.51). However in contrast, when asked how well they think they protected their privacy, the participants' response did not seem to be comparable to their ratings on the level of importance (rated on a 1-5 scale, with 1 as extremely well and 5 as not well at all, mean = 2.65, S.D. = 0.88).

FUTURE RESEARCH

Our future research is designed in two parts; in the first part we define the salient dimensions of privacy based on the literature and the data that we collected as a part of this

project. To understand people's privacy expectations, we ask users to rate the importance of privacy along each of the dimensions that we define i.e., workplace, health-related information, financial information, relationship with partners, children's information, children's performance in academics/sports personal information, political affiliation, religion, online activities, location/schedule information, conversation-related information, home address and other personal identifying information, personal environment, and the contents of digital devices. We also ask users to specify dimensions of privacy that we may not have gleaned from our data.

In the second part of our study we test the relation between privacy and utility. Most of the past work has been done on the monetary value of privacy disclosures. Our goal is to understand the psychological drivers related to voluntary privacy disclosures. We design a series of scenarios around different dimensions of security and provide subjects with scenarios where privacy could be violated along with motives to disclose confidential information, i.e., curiosity, greed, fame, popularity, benevolence, etc. Please note that the focus of this work is not on malicious disclosure of information, which has already been examined extensively (Goel et al. 2017; Zavoyskiy et al. 2018) but on disclosure of information without malicious intent.

CONCLUSIONS

Privacy paradox is a well-articulated phenomenon wherein users profess a need for privacy and yet disclose their private information readily. Our goal is to understand user interpretations of privacy, define contextual dimensions of privacy, evaluate the salience of these dimensions based on user preferences, and then understand the privacy/utility link across these dimensions. In this study, we found that although peoples' definitions of privacy in most domains are quite consistent, their perceived importance of these domains vary. We also obtained a clearer picture about the domains in which people might be concerned about their

privacy. Therefore, we lay the groundwork for our research goals by attempting to delineate the important dimensions of privacy by collecting data from average users. We then present our research design based on the dimensions of privacy gleaned from the data.

REFERENCES

Acquisti, A., 2004. Privacy in electronic commerce and the economics of immediate gratification. In: EC '04 Proceedings of the 5th ACM Conference on Electronic Commerce, USA, 21-29.

Acquisti, A., Grossklags, J., 2005. Privacy and rationality in individual decision making. IEEE Secur. Priv. 3 (1), 26–33.

Baek, Y.M., 2014. Solving the privacy paradox: A counter-argument experimental approach. Comput. Hum. Behav. 38, 33–42.

Barnes, S.B., 2006. A privacy paradox: Social networking in the United States. First Monday, 11(9). Retrieved from http://firstmonday.org/article/view/1394/1312.

Culnan, M.J., Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organ. Sci. 10 (1),340–347.

Deuker, A., 2010. Addressing the privacy paradox by expanded privacy awareness – the example of context-aware services. In: Bezzi, M., Duquenoy, P.,Dienlin, T., Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. 45 (3), 285–297.

Dinev, T., Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. Inf. Syst. J. 17 (1), 61–80.

Donnenwerth, G.V., Foa, U.G., 1974. Effect of resource class on retaliation to injustice in interpersonal exchange. J. Pers. Soc. Psychol. 29 (6), 785–793.

Extended Abstracts on Human Factors in Computing Systems, France, 811–816.

Fischer-Hüber, S., Hansen, M., Zhang, G. (Eds.), Privacy and Identity Management for Life. Springer-Verlag, Berlin, Heidelberg, pp. 275–283.

Foa, U.G., 1971. Interpersonal and economic resources. Science 171 (3969), 345–351.

Goel, S., Williams, K.J., Zavoyskiy, S., and Rizzo, N. (2017) Using Active Probes to Detect Insiders Before They Steal Data, The 22nd Americas' Conference on Information Systems (AMCIS '16), Boston, MA., Aug. 10-13, 2017.

Green, L., Fry, A. F., & Myerson, J. (1994). Discounting of delayed rewards: A life-span comparison. *Psychological science*, *5*(1), 33-36.

Hughes-Roberts, T., 2012. A cross-disciplined approach to exploring the privacy paradox: explaining disclosure behaviour using the theory of planned behavior. In: UK Academy for Information Systems Conference Proceedings, Paper 7.

Hughes-Roberts, T., 2013. Privacy and social networks: Is concern a valid indicator of intention and behaviour?. In: International Conference on Social Computing, Washington, D.C., USA, 909–912.

Identity in the Information Society. Springer-Verlag, Berlin Heidelberg, pp. 226–236.

Joinson, A.N., Reips, U.-D., Buchanan, T., Paine Schofield, C.B., 2010. Privacy, trust, and self-disclosure online. Hum.-Comput. Interact. 25, 1–24.

Kahneman, D., 2003. Maps of bounded rationality: Psychology for behavioral economics. Am. Econ. Rev. 93 (5), 1449–1475.
Kahneman, D., Tversky, A., 1979. Prospect theory: an analysis of decision under risk. Econometrica 47 (2), 263–291.
Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., Greer, C., 2013. Information disclosure on mobile devices: R-examining privacy calculus with actual user behavior. Int. J. Hum Comput Stud. 71, 1163–1173.
Li, H., Sarathy, R., Xu, H., 2010. Understanding situational online information disclosure as a privacy calculus. J. Comput. Inf. Syst. 51 (1), 62–71.
Li, Y., 2012. Theories in online information privacy research: a critical review and an integrated framework. Decis. Support Syst. 54, 471–481.
Manier, M.J., O'Brien Louch, M., 2010. Online social networks and the privacy paradox: a research framework. Issues Inf. Syst. XI (1), 513–517.
Nagy, J., Pecho, P., 2009. Social networks security. In: Third International Conference on Emerging Security Information, Systems and Technologies. IEEE, Athens/Glyfada, Greece, pp. 740–746.
Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: personal information disclosure intentions versus behaviors. J. Consum. Affairs 41 (1), 100–126.
Pentina, I., Zhang, L., Bata, H., Chen, Y., 2016. Exploring privacy paradox in information-sensitive mobile app adoption: a cross-cultural comparison. Comput. Hum. Behav. 65, 409–419.
Pötzsch, S., 2009. Privacy awareness: a means to solve the privacy paradox? In: Vashek, M., Fischer-Hübner, S., Cvrcˇek, D., Švenda, P. (Eds.), The Future of
Pötzsch, S., Wolkerstorfer, P., Graf, C., 2010. Privacy-awareness information for web forums: Results from an empirical study. In: Proceedings: NordiCHI2010, Reykjavik, Iceland, 363–372.
Rachlin, H., & Raineri, A. (1992). Irrationality, impulsiveness, and selfishness as discount reversal effects. In G. Lowenstein & J. Elster (Eds.), *Choice over time* (pp.93-118). New York: Sage.
Simon, H.A., 1955. A behavioural model of rational choice. Q. J. Econ. 69 (1), 99–118.
Smith, H.J., Dinev, T., Xu, H., 2011. Information privacy research: an interdisciplinary review. MIS Quarterly 35 (4), 989–1015.
Sundar, S.S., Kang, H., Wu, M., Go, E., Zhang, B., 2013. Unlocking the privacy paradox: Do cognitive heuristics hold the key?. In: Proceedings of CHI'13.
Tsai, J., Cranor, L., Acquisti, A., Fong, C., 2006. What's it for you? A survey of online privacy concerns and risk. NET Institute Working Paper, No. 06–29, 1–20.
Tversky, A., Kahneman, D., 1975. Judgment under uncertainty: Heuristics and biases. Utility, Probability, and Human Decision Making. Springer, TheNetherlands.
Yoo, C.W., Ahn, H.J., Rao, H.R., 2012. An exploration of the impact of information privacy invasion. In: Proceeding of Thirty Third International Conference on Information Systems, Orlando, Florida, 1–18.
Zavoyskiy, S., Rizzo, N., Goel, S., and Williams, K. Over-claiming as a Predictor of Insider Threat Activities in Individuals, Proceedings of the 9th Workshop on Information Security and Privacy (WISP), December 2018, San Francisco, US.