4-14-2014

Trust and Decision Making in the Privacy Paradox

John-David Rusk
Kennesaw State University, jrusk5@students.kennesaw.edu

THE PRIVACY PARADOX: TRUST AND DISTRUST AS SEPARATE MEDIATING VARIABLES

John-David Rusk
Kennesaw State University
jrusk5@students.kennesaw.edu

ABSTRACT

Privacy has been described as the right to be left alone. In the information age this translates into an individual's right to keep personal or sensitive information private. The privacy paradox is a situation wherein an individual professes a certain level of concern for privacy then discloses personal private information in apparent contradiction to the previously stated privacy concerns. Studies have attempted to explain this paradox through variables including affect, personality, trust, and varied demographic measures. This study attempts to explain further the privacy paradox by including distrust as a variable distinct from the measurement of trust. A model is proposed utilizing trust and distrust as separate mediators between privacy concerns and willingness to disclose. A proposed methodology is provided to continue this research.

Keywords

Trust, distrust, privacy concerns, privacy paradox, willingness to disclose

INTRODUCTION

In today's world of seemingly always online ubiquitous computing, it seems we lose a little bit of control over our private information every time we connect to the Internet. Most of us regularly disclose small portions of our personal information in exchange for relatively small benefits in return. Our level of trust in the recipient of our disclosed information makes a difference in our willingness to disclose personal information. Perhaps our level of distrust will also change our degree of willingness to disclose personal information.

The information age has exacerbated concerns of how personal information is so easily collected, stored, processed, and utilized. Users of ubiquitous computing have sometimes realized they are actually customers of firms that collect their personal information for dubious purposes. These customers have become deeply interested in the topic of information privacy (Pavlou, 2011). An example of this is the October 23, 2013 stable release of the Mozilla Firefox add-on Lightbeam. According to Mozilla:

> Not all tracking is bad. Many services rely on user data to provide relevant content and enhance your online experience. But tracking can happen without the user's knowledge. That's not okay for some. It should be you who decides when, how and if you want your browsing data to be shared. We recognize the importance of transparency and our mission is all about empowering users — both with tools and information.

Mozilla's Lightbeam uses a visualization layout to reveal to the browser user all the known and, until now, unknown entities tracking your browsing experience (Lightbeam for Firefox, 2013).

Information privacy is increasingly becoming an important issue for online consumers. A recent poll by Consumer Reports as reported by Smith, Dinev, and Xu (2011) found 72% of online consumers were concerned their actions were being tracked and profiled (Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy, 2008). A keyword search of the term *privacy* at Google's Android Apps store yielded a results page with several dozen Android applications designed to add additional privacy protection to Android devices. A few of the applications showed download totals over 1,000,000 times each with two applications having been downloaded over 10,000,000 times each (Google Play Apps Search, 2013).

Many people say they want privacy then offer their personal private information online in exchange for a relatively small benefit. This is referred to in the literature as the privacy paradox. How can we understand the difference between an individual's long-term desire for privacy and their insistence on short-term instant gratification? From mobile applications that can track the user's location to Internet connected video game systems so sophisticated that they can read the game players facial expressions and even understand the player's mood, people give away or trade away more information or a regular basis than they might realize (Microsoft Corporation, 2013).

This study seeks to determine if trust and distrust will be distinct from each other as mediators in a model of the privacy paradox using privacy concerns as the independent variable and willingness to disclose as the dependent variable.

PRIVACY CONCERNS

The conceptualization of information privacy has different meanings across different disciplines. In the law literature, information privacy is treated as a right or an entitlement. In the social literature, information privacy is treated as a measure of isolation or a state of limited access. In much of the information systems literature, information privacy deals with an individual's ability to control information about themselves (Smith et al., 2011). Bélanger and Crossler (2011) studied attitudes toward information privacy, including privacy in general, privacy practices, and attitude toward other people. Their study found the variety of information privacy attitudes makes it difficult to have a single stream of privacy research literature.

As reviewed by Smith et al. (2011), general privacy in the U.S. can be traced back to Warren and Brandeis' (1890) article in the Harvard Law Review where general privacy is defined as "the right to be left alone." In their review of several studies, Bélanger and Crossler (2011) categorized four dimensions of privacy: privacy of a person, behavior privacy, communication privacy, and data privacy. In this information age, where much communication and most data are in electronic format they argued that personal communication and data privacy could be merged into information privacy. Smith et al. (2011) find the concept of information privacy varies so widely from discipline to discipline that a single definition could not be sufficient for all areas. They further differentiate information privacy from other related concepts such as anonymity, secrecy, confidentiality, security, and ethics. Privacy has been studied in the fields of information systems, behavioral economics, social networking, and many others disciplines.

WILLINGNESS TO DISCLOSE

Privacy has also been described as the ability to control one's personal information although there has been little agreement among the various fields as to this definition of privacy (Pavlou, 2011). Discussion over how best to allow individual control over provided personal information suggests either granting the individual consumer the right to manage his or her own privacy or governmental legislation to control organizational practices of personal information management. The existence of the privacy paradox suggests individual consumers may not be able to manage their own privacy sufficiently even if afforded the opportunity. Government intervention might be the only truly viable solution (Acquisti and Grossklags, 2005).

Even what many people might consider as reputable firms such as Google, Yahoo, Microsoft, and Facebook share the personal information collected from customers with hundreds of partner companies (Smith et al., 2011). Customers are becoming increasingly more aware of the privacy concerns facing the personal information they disclose. Suggestions have been made to offer customers more control over the storage and sharing of their personal information in an effort to alleviate their privacy concerns and open the customers to share even more intimate information willingly. One noted disadvantage of this for businesses is that once the customer feels they have more control over their own privacy they will share their information with more entities thus watering down the value of their personal information (Pappas, Giannakos, Kourouthanassis, and Chrissikopoulos, 2013).

Hong and Thong (2013) found in their study of online customers that control or loss of personal information is a key component of a customer's interaction with a website. This study supported the concept that customers deem control of personal information important in some situations but not in others. Their study found customers felt the release of personal information important in their interaction with websites but also they had little control over how their information would be managed once released. Customers are more willing to release personal information if they feel they will have control over the management of their information.

When asked if anyone else besides the online merchant would have access to any of the personal information entered in an online credit-card transaction, 34.5 percent of respondents failed to list their own bank. Knowledge the respondents have in their memory seems to be unavailable to them during the survey and perhaps at the point of making the decision whether to disclose personal information for an online purchase as well. Customers so quickly give up their privacy by trading their personal information for such low immediate benefits. Yet these actions can have profound effects lasting for a longer time than expected and, in extreme cases, the damage may be permanent (Acquisti and Grossklags, 2005).

PRIVACY PARADOX

The privacy paradox is a situation where an individual claims to have high concerns over the release of personal information then, in opposition to their own stated stance, the individual releases sensitive personal information for relatively small benefits. Acquisti and Grossklags (2005) found that although their respondents showed sophisticated privacy attitudes over 87% of individuals in their sample confessed they had disclosed real personal information to join loyalty programs then declared they had never disclosed personal information for monetary or other rewards. They also found over 20% of respondents acknowledged disclosing their social security numbers for discounts or better services or recommendations.

While these seem to be opposite actions, it does not imply this is irrational behavior. Willingness to disclose decisions are based on the final conclusion of various facts, attitudes, and cost-benefit analyses. This is the privacy paradox where individuals claim to value privacy then disclose personal information in ways that seem contrary to their privacy claims. Could measures of trust and distrust as separate variables help explain this apparent privacy paradox?

People who claim to keep their personal information private readily disclose their personal information for seemingly small benefits. Personal information is traded as a commodity for some trifle value in return. One such popular benefit is personalized consumer advertising. Smith et al. (2011) propose three major types of information privacy disclosure benefits 1) financial rewards 2) personalization 3) social adjustment benefits. Customers assert they do not want to share their personal information but find they must in order to get the benefits of personalized services. Yet, for the information to be shared voluntarily there must also be some level of trust that the information will be handled appropriately by the service provider (Pappas et al., 2013).

A specialized situation of the privacy paradox is called the personalization privacy paradox. According to Lee and Cranage (2011), personalization is defined as the e-business practice of fitting products, services, advertising, and recommendations to specific customer preferences. This personalization creates a perceived value for the customer that tends to lead to positive attitudes about the service. In order to obtain these benefits the customer must release personal information. Doing so causes the customer to experience privacy concerns about the disclosure of such information. The thought of their personal information being collected, tracked, and stored without their consent causes negative feelings toward the service. Customers find they are caught in a personalization privacy paradox between the benefits of personalization and the risk of exposure because the personal information disclosed most certainly may be released without their control. Empirical evidence shows customers consider highly personalized advertising as proof their browsing and purchase history privacy has been invaded.

TRUST

Trust is a vital component in any transactional relationship between a customer and a business, particularly when the human factors of interaction where trust is traditionally built are replaced by computerized online interactions. Because an online business can easily take advantage of its online customers, businesses must find other ways to build trust (Gefen et al., 2003). Any feelings of trust created or developed in the customer's view of the business can ease privacy concerns, promote the sharing of personal information, and facilitate the completion of a transaction. It is reasonable to expect that trust encourages positive attitudes toward sharing information and that trust and privacy concerns will be negatively correlated (Lee and Cranage, 2011).

Customer trust in a business is affected by comparing the benefits and costs that accrue to the business when it cooperates in a healthy long-term customer relationship against the costs and benefits incurred to the business when it cheats in the relationship. When a business's costs of cheating the customer outweigh the benefits of cheating the customer, the customer will develop trust in the business since cooperation in the relationship is in the business's own interest. In general, one party's trust increases when the other party's untruthfulness leads to potential losses (Gefen et al., 2003).

Any opportunistic behavior, whether legal or not, erodes customer trust. Online business must continually maintain and rebuild customer trust (Gefen et al., 2003). Any breach of trust will hurt the business by causing privacy concern fears to increase in the customer thereby reducing the likelihood of a completed transaction (Schwaig, Segars, Grover, and Fiedler, 2012).

DISTRUST

A customer who releases personal information to a business may not know what that business might do with the collected data. When uncertainty exists, trust becomes a determinant of how a customer would expect a business to handle the customer's personal information. When a firm can take advantage of a customer by using the customers personal information in ways in which the customer did not agree trust becomes an issue. This is particularly true in the case of online vendors where so much of the customer's personal information is in the control of the online vendor (Gefen, Karahanna, and Straub, 2003).

Acquisti and Grossklags (2005) found 83.5% of e-commerce participants believed it is very likely or most likely that their personal information disclosed would be used for marketing purposes by the online vendor. They further found 76% believed it quite likely or very likely a third party could monitor some usage details of a file sharing client.

Pappas et al (2013) on page 46 found no significant relationship between trust and anxiety where Hwang and Kim (2007) found a negative relationship. If this discrepancy is due to the differences in the instruments used then this field would be better served by a standard instrument to measure the variables. If this discrepancy is due to the models measuring trust without measuring distrust then future studies should include distrust as a separate variable.

Perhaps the difference is in the definition of trust. Marsh (1994) defined trust as a measure from indifference to total trust, and conversely, distrust as a measure of indifference to total distrust. The result: trust, lack of trust, and distrust are three separate states of trusting behavior. Hong and Thong (2103) call for the need to use consistent measures for dimensions of internet privacy concerns.

Some studies measure trust in a manner that combines questions that measure trust with questions that potentially measure distrust with both items anchored to the same seven-point scale that ranges from strongly disagree to strongly agree (Malhotra, Kim, and Agarwal, 2004). Marsh (1994) recommends the variables of trust and distrust be measured separately. Depending on the wording of a particular item, the lack of trust can only be measured as indifference and not, as could be interpreted in some cases, distrust.

McKnight and Choudhury (2006) verified beliefs and intentions of trust and distrust can be distinct variables operating as mediators between structural assurance and various intentions in an e-commerce model. Additional research needs to be conducted to determine more specifically how trust and distrust are related, how they are distinct, and what this means to businesses. The measure of trust and the measure of distrust are required because they measure different attitudes of a situation. According to the definitions of this model, trust and distrust are equal when both equal zero. When this occurs, there is a state of indifference. (Marsh 1994)

MODEL

Trust is studied both as an antecedent of privacy and as an outcome of privacy. Trust has been studied as a moderator of the effects of privacy on behavior and as a mediator between privacy concerns and willingness to disclose private information. Studies have shown trust is an interrelated variable to information privacy, but just how that relationship is defined is still open to debate (Pavlou, 2011; Smith et al., 2011). Still others do not look at trust independently, but as an underlying relationship affecting constructs such as data transparency and information policies (Awad and Krishnan, 2006).

In privacy models, trust has been used as an independent variable (Hong and Thong, 2013; Pappas et al., 2013) as well as a dependent variable (Hwang and Kim, 2007). It has been included as a mediator (Dinev and Hart, 2006; McKnight and Choudhury, 2006; Metzger, 2004), and as a control variable (Sutanto, Palme, Tan, and Phang, 2013). Far less research has been devoted to the specific study of distrust. Much research methodologies measure trust without measuring distrust separately (Pappas et al., 2013) while other methodologies treat distrust as a separate variable altogether (McKnight and Choudhury, 2006). A typical use of trust as a mediator between privacy concerns and willingness to disclose is shown in Figure 1.

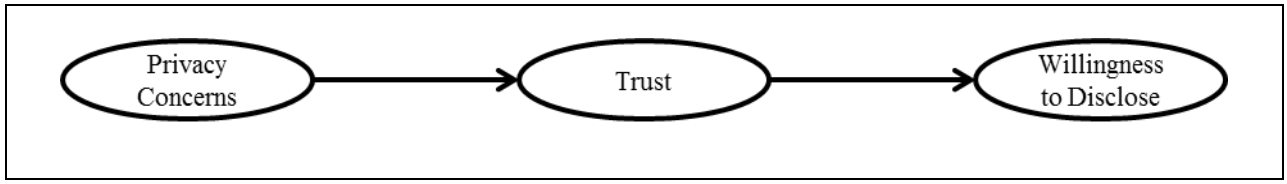

Figure 1. The model without Distrust

Smith et al. (2011) find numerous normative studies to explain how different constructs should relate to information privacy. More empirical studies that focus on the actual outcomes of privacy concerns may explain the why of information privacy issues. Previous research has studied trust as a mediator between an individual's view of information privacy and willingness to disclosure personal information. This paper proposes a study to test the relationships of trust and distrust as separate mediators between privacy concerns and willingness to disclose in the privacy paradox. The proposed model for this study is shown in Figure 2.

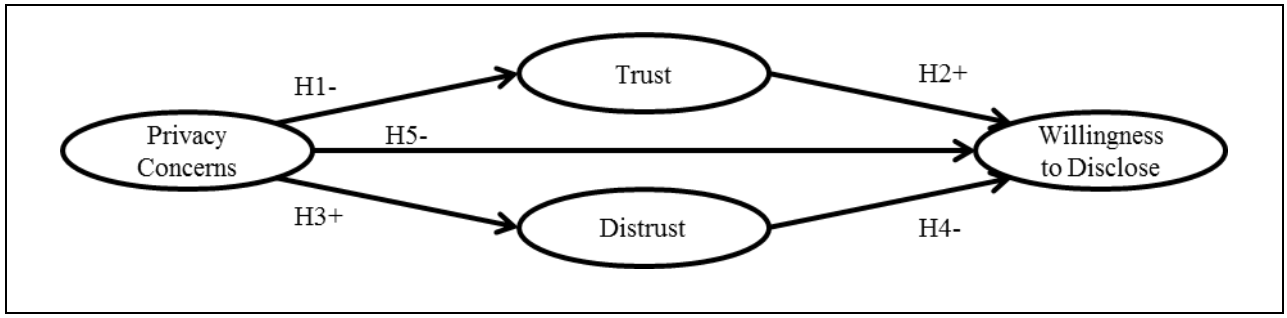

Figure 2. The proposed model with trust and distrust as separate variables

HYPOTHESES

Hypothesis 1: Higher Privacy Concerns are related to lower levels of Trust.

Hypothesis 2: Higher levels of Trust are related to a higher Willingness to Disclose.

Hypothesis 3: Higher Privacy Concerns are related to higher levels of Distrust.

Hypothesis 4: Higher levels of Distrust are related to lower levels of Willingness to Disclose.

Hypothesis 5: Higher levels of Privacy Concern are related to a lower Willingness to Disclose

FUTURE INTENTIONS

The plan to proceed with this study of trust and distrust is to test the proposed model by following the steps outlined here. A list of trust and distrust instrument items will be compiled from previous research. This list will be condensed with help from area experts and tested through structural equation modeling with data collected from student samples. Once the new instrument is shown to have discriminant validity between the trust and distrust constructs and convergent validity overall, new data will be collected from a more diverse population.

CONCLUSION

Ten years have passed since the 2003 article by Gefen et al. where research found that trust, with an underlying component of privacy assurance, is an excellent predictor of online shopping behavior. Since the introduction of smartphones, tablets, and other ubiquitous computing devices, the need is greater for more attention to be focused on information privacy concerns. Many popular laptops, tablets, smartphones, and other electronic devices are built with location awareness, fingerprint readers, thermometers, barometers, and various other sensors that generate and collect vast amounts of data. Even Internet enabled video game systems are becoming sophisticated enough "to see where the user is, what they are doing, read user facial expression, even mood" (Microsoft Corporation, 2013). The widespread connectivity of these systems means almost constant monitoring of customers with personally identifiable information available for live streaming to be stored, processed, and shared at any time (Ackerman, 2004). A privacy model measuring trust and distrust may help to understand better the privacy paradox that exists.

Concerns for information privacy are increasing due to the voluminous amounts of personal information being collected, transmitted, and indefinitely stored (Hong and Thong, 2013). As customers continue to make online purchases where private information is gathered and continue to use mobile applications that discover the customer's most personal information, the question becomes "Is free worth the price, if privacy is the cost?" Understanding the privacy paradox may help answer this immensely important question. The answer of whether distrust should be considered whenever trust is considered can help businesses know when to invest more in building trust and when to invest more into the elimination of distrust.

REFERENCES

1. Ackerman, M. S. (2004) Privacy in pervasive environments: Next generation labeling protocols, *Personal and Ubiquitous Computing*, 8, 6, 430–439.

2. Acquisti, A., and Grossklags, J. (2005) Privacy and rationality in individual decision making, *Security & Privacy, IEEE*, 3, 1, 26–33.

3. Awad, N. F., and Krishnan, M. S. (2006) The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization, *MIS Quarterly, 30, 1, 13-28.*

4. Bélanger, F., and Crossler, R. E. (2011) Privacy in the digital age: A review of information privacy research in information systems, *MIS Quarterly*, 35, 4, 1017–A36.

5. Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy. (2008, September 25). Retrieved from Consumers-Union: http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html

6. Gefen, D., Karahanna, E., and Straub, D. W. (2003) Trust and tam in online shopping: An integrated model, *MIS Quarterly*, 27, 1, 51–90.

7. Google Play Apps Search. (2013, 10 29). Retrieved from Google Play: https://play.google.com/store/search?q=privacy&c=apps

8. Hong, W., and L. Thong, J. Y. (2013) Internet privacy concerns: An integrated conceptualization and four empirical studies, *MIS Quarterly*, 37, 1, 275–298.

9. Hwang, Y., & Kim, D. J. (2007). Customer self-service systems: The effects of perceived Web quality with service contents on enjoyment, anxiety, and e-trust. *Decision Support Systems*, 43(3), 746-760.

10. Lee, C. H., and Cranage, D. A. (2011) Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites, *Tourism Management*, 32,5, 987–994.

11. Lightbeam for Firefox. (2013, 10 23). Retrieved from Mozilla: http://www.mozilla.org/en-US/lightbeam/

12. Marsh, S. (1994, October). Optimism and pessimism in trust. In Proceedings of the Ibero-American Conference on Artificial Intelligence (IBERAMIA'94).

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

14. McKnight, D. H., & Choudhury, V. (2006, August). Distrust and trust in B2C e-commerce: Do they differ?. In Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet (pp. 482-491). ACM.

15. Microsoft Corporation. (2013, August 11). Software Development Engineer-IEB-Kinect 4 Windows (807940). Retrieved October 17, 2013, from Microsoft Careers: https://careers.microsoft.com/resumepreview.aspx?aid=91885

16. Pappas, I. O., Giannakos, M. N., Kourouthanassis, P. E., and Chrissikopoulos, V. (2013) Assessing emotions related to privacy and trust in personalized services, *International Federation for Information Processing*, 38–49. Retrieved from Springer: http://link.springer.com/chapter/10.1007/978-3-642-37437-1_4

17. Pavlou, P. A. (2011) State of the information privacy literature: Where are we now and where should we go, *MIS Quarterly*, 35, 4, 977–988.

18. Schwaig, K. S., Segars, A. H., Grover, V., and Fiedler, K. D. (2012) A model of consumers' perceptions of the invasion of information privacy, *Information & Management, 50, 1-12.*

19. Smith, H. J., Dinev, T., and Xu, H. (2011) Information privacy research: An interdisciplinary review, *MIS Quarterly*, 35,4, 980–A27.

20. 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).

21. Warren, S. D., and Brandeis, D. L. (1890). The right to privacy. *Harvard Law Review*, 4:5, 193-220.