Heather Shoenberger, JD, P.h.D; hshoenbe@uoregon.edu; 8458201181
Jasmine McNealy, JD, P.h.D; jmcnealy@ufl.edu, 3528460226

ABSTRACT

Offline v. Online: Re-examining the Reasonable Consumer Standard In the Digital Context

Overview

According to the Federal Trade Commission, "Every Web site where data is collected for behavioral advertising should provide a clear, consumer-friendly, and prominent statement that data is being collected to provide ads targeted to the consumer and give consumers the ability to choose whether or not to have their information collected for such purpose (FTC 2007)." This study tackles the questions of whether a consumer has a realistic opportunity in today's digital context to wield control over her data online or if the "reasonable consumer" needs redefining and the development of new methods of notice and choice to address the social norms online. We argue the combination of consumer lack of self-protective measures regarding data collected by any digital privacy promising system (any application, advertisement, or website that uses consumer data) and the current method of notice and choice offered leave consumers with no meaningful notice or choice regarding the way their data are used online. Our exploration is especially important to applications, websites, social media and advertisers looking to make use of the audiences and data about those audiences that exist online to serve better, more relevant advertising and products/services.

We also aim to fill in the gaps in the literature noting the reasons for the seemingly nonchalant consumer online. Previous theorizing has offered explanations for consumer behavior in the online context suggesting that consumers navigate the online environment via a complex calculation of risks and benefits and/or an existing social contract (e.g., Okazaki, Li & Hirose, 2009; Malhotra, Kim & Agarwal, 2004). Most importantly, many offline understandings of behavior have been applied to online behavior as well (see Beldad, de Jong & Steehouder (2010) for an explanation of differences in the variable of trust offline versus online). Our study suggests that consumers rarely consciously weigh the costs and benefits when interacting with privacy-promising technologies (e.g., Snapchat, Facebook, online retail sites) and behave in ways that are different than they would offline in regards to issues of privacy. We attempt to examine what is considered "reasonable" data protection behavior.

Overarching research questions

RQ1: What are the parameters of the concept of control over one's data online according to consumers?
RQ2: What are consumers' privacy expectations online versus offline?
RQ3: What bad experiences, if any, have consumers had when using an application or online retailer's site?

RQ4: Will peer recommendation be linked to perception of control over one's data, lower expectations of privacy, and higher likelihood to simply click on the box indicating one has accepted the terms of agreement for the particular application or e-retailer recommended?

Literature Review:

This brief literature review sets up our overarching research question, which is whether the definition of the reasonable person as defined by the Federal Trade Commission in regards to privacy promising technologies needs to be amended to address the majority of consumer behavior online. We argue the way that people behave online is fundamentally different than the way they behave in the brick and mortar world. We theorize that, for the most part, consumers are operating online on mental auto-pilot, allowing previous knowledge structures developed from past experiences to guide their behavior. Our study sits amidst prior research that puzzle over the lack of attention paid to privacy policies, a culture of apathy towards such policies, and attempts to fill in the gap in the literature as to why that might be.

According to the Federal Trade Commission, "Every web site where data is collected for behavioral advertising should provide a clear, consumer-friendly, and prominent statement that data is being collected to provide ads targeted to the consumer and give consumers the ability to choose whether or not to have their information collected for such purpose" (FTC, 2007). Many applications collect user data and may have terms of agreement, privacy promises that pop up as legalese just before a consumer downloads or uses an application.

Currently, what does the reasonable consumer pay attention to as far as privacy policies online? Many studies suggest; not much if anything at all. Consumers consistently indicate a desire for privacy protections yet show little interest in attending to such policies, rarely taking proactive measures to control their data (Joinson, Reips, Buchanan & Schofield, 2010; Metzger, 2007). While previous studies suggest consumers want more privacy policies in the digital context, (McDonald & Cranor 2010; Turow et. al., 2009), according to a recent White House report, consumers nearly always click on terms of agreement without reading them, adding incentive for privacy advocates and researchers to wonder whether the opt-out system and current privacy policies are effective at ensuring consumers have adequate notice and choice over the use of their data (Sanger & Lohr 2014; Leon, Ur, Shay, Wang, Balebako & Cranor, 2012).

In the realm of websites collecting consumer data for advertising, in an effort to prevent the creation of Federal Trade Commission regulations, the advertising industry has worked to provide regulatory logos on advertisements generated through the use of consumer online behavioral data based on the FTC's notice provision based on the idea that consumer control over data is a foundation of privacy (Sheehan & Hoy, 2000). Unfortunately, the logos have led consumers to rely on them as safety heuristics much like the *Good House Keeping* seal of approval and their ability to motivate consumers to understand the ways in which their data are being handled has not been successful (LaRose & Rifon, 2007). The use of icons and privacy policies as heuristics adds fodder to our argument that heuristics or mental short-cuts are at work when consumers are interacting with privacy promising digital technologies but leaves a gap in the literature as to where the boundaries of consumer privacy concerns may lie online and why they may rely on heuristics almost entirely when downloading applications and surfing on the Internet. In some cases, we argue peer usage/recommendation may override any concern for privacy issues and serve as a compelling heuristic denoting safety of a privacy promising technology. For example, Snapchat users were asked if they knew their snaps could be captured and saved. About eighty percent of the people asked indicated that they were aware that snaps could be captured and just over fifty percent noted that they didn't care (Roesner, Gill & Kohno, 2014). We also realize that some intervening issues such as previous bad experiences may enter into the equation and we plan to include that and other issues that arise in our interviews in the finalized version of our survey.

Based on this short review we find a reasonable person who is especially vulnerable to deceptive and misleading practices by privacy promising technologies. There appears to be little regard by the consumer for the privacy details offered, particularly when considering technologies with an element of entertainment such as a shopping website or Snapchat. If a company relies on the fine print for a consumer to figure out that their information could be used in a way that is not in line with their expectations of the application – no matter where that expectation arose (e.g., peers, advertising for the privacy promising technology, etc.) – the reasonable consumer is vulnerable to deception/misleading information in this special context. We seek to gather empirical data from consumers themselves about the social norms that have been created online, how people imagine their privacy expectations online, and offer policy makers an argument to potentially revise the current "reasonable consumer" standards for the Internet to avoid the misuse and potential embarrassment of our ever more intrusive mechanisms for sharing content in the digital context.

Proposed Methods:

Part one: Individual interviews were performed and are currently being analyzed (N=30). The resulting information and vocabulary used by the participants will inform the wording and type of questions used in part two of the study in addition to the questions already established.

Part two: A survey (N=1000) will be conducted via Amazon's M-Turk to examine our overarching research question: whether the definition of the reasonable person as defined by the Federal Trade Commission in regards to privacy promising technologies needs to be amended to address the majority of consumer behavior online. Previous research indicates that MTurk participants produce reliable results that are consistent with previous decision-making research (Goodman, Cryder, & Cheema 2012) and exhibit similar judgment and decision biases compared with online discussion board participants (Paolacci et al. 2010). Additionally, Buhrmester et. al. (2011) assert that MTurk participants are more demographically diverse and more representative of non-college populations than those of typical Internet and traditional convenience samples. The ease of MTurk allows for over-sampling in the case that some of the participants have to be removed due to incomplete questionnaires or insincere participation. Safeguards will be put in place in an effort to ensure attention paid to the survey (text entry questions) and questions addressing nationality to ensure United States' residents are those included in the dataset.

Interviews

Thirty minute semi-structured interviews were aimed at addressing the aforementioned research questions. The basic format will follow the research questions. For example, "Would you show a new acquaintance a photo album in your home? How many people on social media are acquaintances? Do you manage the privacy settings on photos you post?" The purpose of the interviews is to gain vocabulary used by the consumer when talking about privacy promising digital technologies and to uncover behaviors that may vary between offline and online privacy concerns. Participants were recruited from a Southeastern community and a Northwestern community via advertisement.

Questionnaire

The survey will be administered via Qualtrics survey software. The items will be designed to tap into each concept of interest. Most will be informed by the individual interviews. Some examples of the items asked will deal with privacy expectations online versus offline – tapping into the potential for different social norms online versus offline. For example, "When people I've just met come to my home, I show them photos from previous vacations." "Many people who follow my social media sites are people I do not personally know." "When I am at a store and the clerk asks for my email address I give it readily." Other items address another facet of social norms online, the peer recommendation/influence such as: "If a friend has an app, I will download it." "When a friend is using an app, I assume the app is safe." "I assume shopping at known online stores is safe." Vocabulary online versus offline is addressed (e.g., a "friend" online vs. "friend" offline). We examine the concept of over data online: "When I download an application, I click the terms of agreement without reading." Perceived versus actual control over consumer data online is addressed. Previous bad experiences with data online will be examined via open-ended and scale items. Most items (except demographic items) will be asked in random order to mitigate order effects. Other items address what consumers see as a reasonable way to control their data online via open-ended questions and scale items. All items from scales created for this study will be submitted to exploratory factor analyses where appropriate.

Analyses

Grounded theory will be employed to derive themes from open-ended questions and interview responses. Survey data will be analyzed by multiple regressions to address the hypotheses resulting from our interview data and previous research. Analyses of variance will be used to determine differences in indicated behaviors online and offline in regards to expectations of privacy and control over one's data from the survey responses.

Findings:

We will present the results from our interviews and the following survey. Preliminary analyses of the interviews lend us to the speculate on policy considerations and further study in an attempt to offer an explanation and empirical evidence of why consumers should be considered particularly vulnerable in the digital context when it relates to any privacy-promising online technology that uses consumer data.

References

Beldad, A., De Jong & Steehouder. (2010). "How Shall I Trust the Faceless and the Intangible? A Literature Review on the Antecedents of Online Trust." *Computers in Human Behavior*. 26, 5. 857-869.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data?. *Perspectives on psychological science*, *6*(1), 3-5.

Consumer Data Privacy In a Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Digital Global Economy. 2012. Available from http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Goodman, J. K., Cryder, C. E., & Cheema, A. (2013). Data collection in a flat world: The strengths and weaknesses of Mechanical Turk samples. *Journal of Behavioral Decision Making*, *26*(3), 213-224.

Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, *25*(1), 1-24.

Leon, P., Ur, B., Shay, R., Wang, Y., Balebako, R., & Cranor, L. (2012, May). Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 589-598). ACM.

Malhotra, N. K., Kim, & Agarwal (2004). "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." *Information Systems Research.* 15. no. 4. 336-355.

McDonald, A. M., & Cranor, L. F. (2010, October). Americans' attitudes about Internet behavioral advertising practices. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society* (pp. 63-72).

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer‐Mediated Communication*, *12*(2), 335-361.

Okazaki, S., H. Li, & M. Hirose. (2009). "Consumer privacy concerns and preference for degree of regulatory control." *Journal of Advertising.* 38. no. 4. 63-77.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on amazon mechanical turk. *Judgment and Decision making*, *5*(5), 411-419.

Podesta, Pritzker, Moniz, Holdren, Zients (2014). "Big Data Seizing Opportunities, Preserving Values." *Executive Office of the President.* Retrieved from: http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

Sanger, D. & Lohr, S. (2014) "Call for limits of web data on consumers." *The New York Times*. Retrieved from: http://www.nytimes.com/2014/05/02/us/white-house-report-calls-for-transparency-in-online-data-collection.html.

Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust insights from a national survey. *New media & society*, *9*(2), 300-318.

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., & Hennessy, M. (2009). Americans reject tailored advertising and three activities that enable it. *Available at SSRN 1478214*.

What They Know. (2010-2012). Retrieved from http://online.wsj.com/public/page/what-they-know-digital-privacy.html.