Computers in Human Behavior 55 (2016) 372–383

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

The effects of attacker identity and individual user characteristics on the value of information privacy

Kenneth D. Nguyen [a, *], Heather Rosoff [b], Richard S. John [a]

[a] Psychology Department, University of Southern California (USC), USA
[b] Center for Risk and Economic Analysis of Terrorism Events, University of Southern California (USC), USA

ARTICLE INFO

Article history:
Received 21 April 2015
Received in revised form
31 August 2015
Accepted 21 September 2015
Available online 30 September 2015

Keywords:
Multi-attribute utility
Trade-off preference
Privacy concern
Privacy attacker identity

ABSTRACT

Past research indicates that people have strong concerns about their information privacy. This study applies multi-attribute utility theory to conceptualize the concern for smartphone privacy and examine how people value smartphone privacy protection. We also investigated how the value of privacy varied by the identity of a privacy attacker and individual user characteristics. Respondents were given a hypothetical choice between an encrypted smartphone and a regular one. The encrypted smartphone increases the level of privacy protection at the cost of lower usability, greater monthly service payments, slower speed, and additional inconvenience. Respondents were asked to simply make binary choices between hypothetical pairs of smartphone configurations. The results show that respondents were willing to make non-trivial sacrifices for smartphone privacy protection. Interestingly, specifying the identity of an attacker collecting information decreased the value of privacy protection compared to not specifying the identity of the attacker. We also observed effects of individual user characteristics, including general privacy concern, age, and self-reported political attitude, on the value of smartphone privacy protection. These results offer greater insight on how people value their privacy.

1. Introduction

Research suggests that people are increasingly concerned about their information privacy (Culnan & Milne, 2001; Gandy, 2003; Gross & Acquisti, 2005; TRUSTe, 2012; Utz & Kramer, 2009). However, these findings have been recently called into question as a number of studies indicate that people are willing to engage in behaviors that increase their information privacy risks despite their stated privacy concerns—a phenomenon known as the "privacy paradox" (see Bélanger & Crossler, 2011 for a review). Baek (2014) argued and presented evidence that the privacy paradox is probably the result of unreliable polling questions, and called for a new scientific approach to examine attitudes and behaviors related to information privacy.

The current research presents a different approach to study privacy concern by quantitatively addressing how people trade their privacy for other valued attributes. This trade-off methodology has its roots in *multi-attribute utility theory* (MAUT), a framework that prescribes how people should evaluate a decision that includes multiple alternatives and multiple conflicting objectives (Keeney & Raiffa, 1993). Conceptually, the trade-off approach is also compatible with the notion of a *privacy calculus* (or *privacy as a commodity*), which has been the subject of extensive research in the information privacy literature (Smith, Dinev, & Xu, 2011). Importantly, the trade-off approach also offers richer information about information privacy concern as part of a broader value system. Surprisingly, despite numerous surveys on information privacy attitude (see Preibusch, 2013 for a review), relatively few studies have been conducted to examine how people trade-off information privacy when there is a conflict with other personal objectives.

Past research suggests that people differ widely in their information privacy attitude (Ackerman & Mainwaring, 2005). Thus, understanding factors associated with diverse views about information privacy is important. Previous research has examined the effects of information privacy concern and demographic factors such as sex, age, and political attitude on privacy-related judgments and behaviors. However, these relationships are often inconsistent between studies, indicating the need for further research to examine these relationships. Furthermore, the role of social contextual factors in understanding information privacy concerns

* Corresponding author. Department of Psychology, University of Southern California, SGM 501, 3620 South McClintock Ave, Los Angeles, CA 90089-1061, USA.
E-mail address: hoangdun@usc.edu (K.D. Nguyen).

http://dx.doi.org/10.1016/j.chb.2015.09.031
0747-5632/

and behaviors are not well-understood. In particular, there has not been a study to examine how people value information privacy policy as a function of the identity of an attacker who collects information for a specific, usually ill-indented, purpose.

The current research attempts to close these research gaps by first examining how people make trade-offs for information privacy in a multi-attribute context in which their privacy concern conflicts with other personal values. Second, we investigate predictors of information privacy trade-offs by examining how demographic variables including sex, age, political attitude, general online privacy concern, and the attacker identity relate to how people make trade-offs for information privacy. Importantly, we examine these research questions in the context of smartphone technology. The context is carefully chosen because a number of surveys indicate that people increasingly worry about the security and privacy of their smartphone data (Chin, Felt, Sekar, & Wagner, 2012; Egelman, Felt, & Wagner, 2012). Smartphone technology also provides a new and unique platform to examine how people evaluate their concern for information privacy against other conflicting objectives that they value such as speed, cost, usability, and convenience.

2. Theory and research questions

2.1. Privacy valuation

The trade-off methodology is an application of the concept privacy calculus. This concept suggests that people disclose their private data when they believe such exchange is essential and yields benefits in return (Culnan & Armstrong, 1999). Results from economic experiments provide support for this notion. Respondents, for example, were willing to trade their personal data for financial gains (Acquisti & Grossklags, 2005), for personalization purposes (Chellappa & Sin, 2005), and for small discounts (Spiekermann, Grossklags, & Berendt, 2001). However, much of the research on the privacy calculus examines the economic value of privacy. This is a research gap because people not only value their privacy and money but they also consider other objectives in making decisions that have implications for their information privacy (Tsai, Egelman, Cranor, & Acquisti, 2011; Workman, Bommer, & Straub, 2008). Importantly, these values are often conflicting in the sense that getting more of one means giving up some amount of the other (Keeney, 1999), and these conflicts often make it harder to understand the role of information privacy concern. Multi-Attribute Utility Theory (Keeney & Raiffa, 1993) provides a theoretical foundation to conceptualize the role of privacy concern in a broader value system. The theory prescribes a quantitative framework that helps individuals resolve a decision problem involving multiple conflicting objectives. The mathematical formulation is expressed as[1]

$$U(X_1, X_2 \ldots, X_n) = \sum_{i=1}^{n} w_i u_i(x_i)$$

"U" is the multi-attribute utility of a decision's outcome; the capital "X" represents the operationalization of an objective, often referred by the term *attribute*—note that multiple Xs represent multiple (conflicting) objectives; the lower case "x" indicates the level of the respective attribute; the indexed "u" represents the utility of a single attribute resulted from the decision's outcome; and "w" is the scaling constant. A decision maker computes the expected (multi-attribute) utility for each alternative and chooses the decision option with the highest utility. The scaling constants are important because they are derived from the subjective judgments of trade-offs between the conflicting objectives. It is this parameter "w" that makes the trade-off methodology particularly important in MAUT. In this research, we apply MAUT to conceptualize how people evaluate their privacy concern in a multi-attribute context. In particular, we define information privacy concern as the trade-off values for privacy protection.

Importantly, the focus of this research is not to construct a mathematical model but rather to understand how people judge the value of information privacy in relations to other attributes. This conceptualization is fruitful because if offers richer information on concerns about information privacy. Using the trade-off method, researchers can understand when people highly value their information privacy, and when they consider information privacy as a minimal concern. For example, using conjoint analysis—a framework that is comparable to the MAUT, Hann, Hui, Lee, and Png (2007) found that website visitors valued privacy more when they traded information privacy for convenience, but they valued information privacy less when they had to trade privacy for monetary rewards.

The use of MAUT to conceptualize information privacy concern is particularly suitable in the context of smartphone technology because smartphone users often have to make many trade-offs for information privacy. Indeed, smartphone users have to sacrifice some levels of information privacy protection to obtained desired levels of other smartphone attributes. For instance, an encrypted smartphone often costs more than a non-encrypted device. The privacy-enhancing Blackphone[2] can cost users about twice the price of other popular smartphones. As another example, some users surely enjoy the convenience of location-based applications, but they also have concerns about the prospect of having their data collected and used for location-based services (Zhou, 2011). This requires users to make a trade-off because these mobile applications often require excessive permission to access user's smartphone data. Therefore, we aim to address the question of how people evaluate their smartphone privacy in a multi-attribute context. Specifically, we are interested in how people trade their preference for a high level of privacy protection for each of the following objectives: maximizing speed, minimizing cost, maximizing usability, and maximizing convenience. These objectives are selected because they conflict with one another, and these objectives are also generally relevant to users' decision making.

We evaluate four information privacy trade-offs by setting up a decision problem that requires respondents to choose between two smartphone alternatives. An encrypted smartphone helps to attenuate information privacy risks (high in privacy), but it is more expensive (high in cost), more difficult to use (low in usability), lengthens the processing time of data transmission (slow in speed), and limits users' access to a number of mobile applications (low in convenience). The alternative smartphone is not encrypted (low in privacy), but it is cheaper, more user-friendly, faster, and allows a greater access to mobile applications. By asking respondents which smartphone they prefer to purchase in various paired choices, we are able to quantify how much sacrifice in each of the attributes, cost, speed, usability, and convenience that users are willing to make for an encrypted smartphone with enhanced information privacy. We refer these trade-off values for privacy as the *privacy premiums* hereafter.

[1] Assuming an additive form.

[2] www.Blackphone.com. The cost for the Blackphone is estimated based on the purchase cost and the monthly subscription fee for, which is not paid when users purchase a non-encrypted smartphone.