The Social Science Journal 51 (2014) 523–533

Contents lists available at ScienceDirect

The Social Science Journal

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

Changing the default setting for information privacy protection: What and whose personal information can be better protected?

Young Min Baek[a,*], Young Bae[b], Irkwon Jeong[c], Eunmee Kim[d], June Woong Rhee[d]

[a] College of Communication, Yonsei University, 50 Yonsei-ro Seodaemun-gu, Seoul 120-749, South Korea
[b] Department of Information Sociology, Soongsil University, 369 Sangdo-ro Dongjak-gu, Seoul 156-745, South Korea
[c] School of Communications, Kwangwoon University, 20 Gwangun-ro Nowon-gu, Seoul 139-701, South Korea
[d] Department of Communication, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul 151-742, South Korea

ARTICLE INFO

Article history:
Received 1 August 2013
Received in revised form 9 July 2014
Accepted 9 July 2014
Available online 31 July 2014

Keywords:
Information privacy
Status quo bias
Framing effect
Loss aversion
Notice-and-consent requirement

ABSTRACT

With Internet service providers (ISPs) increasingly demanding personal information to develop personalized services, people have become more vulnerable to privacy infringement. As a way to protect individuals' privacy, industrialized countries have implemented a "notice-and-consent" requirement, meaning an ISP must obtain users' consent to collect personal information in the course of the ISP's business. Drawing on prospect theory and earlier work on information privacy and behavioral science, in this study, we administered an online survey experiment to test whether the giving of consent differs between 'opt-in' and 'opt-out' frames. The framing effect was found to be moderated by personal information type, people's attitudes toward privacy, and people's privacy infringement experience. The results indicate that the opt-in frame better protects users' information privacy, and the framing effect is magnified when the targeted information concerns online activities, when users have weakly held privacy attitudes, and when users have less experience of privacy infringement.

1. Introduction

In recent years, personalized technologies such as recommendation systems and behavioral targeting have been touted as new engines for the Internet economy (Anderson, 2006; Mayer-Schönberger & Cukier, 2013; The White House, 2012). Such technologies, operated by Amazon, Google AdWords, and other online commercial companies, gather users' personal information to create customized services fitted to users' preferences (Berger, 2010; Goldfarb & Tucker, 2011; Riedl, 2001). For more effective customized services, Internet service providers (ISPs) must collect more personal information. In the Web 2.0 era, personal information has become the fuel of ISPs (Mayer-Schönberger & Cukier, 2013; The White House, 2012).

However, indiscriminate gathering of personal information not only generates annoyances such as spam and marketing calls but can also lead to identity theft or online stalking, destroying people's privacy (Goldfarb & Tucker, 2011; Riedl, 2001). In spite of the convenience of customized services, concerns over unfair or deceptive use of personal information have escalated in industrialized societies (Andrews, 2011; Dinev, Xu, Smith, & Hart, 2013; Hong

* Corresponding author. Tel.: +82 2 2123 2983; fax: +82 2 2123 7642.
E-mail addresses: ymbaek@yonsei.ac.kr, ymbaek@gmail.com (Y.M. Baek).

http://dx.doi.org/10.1016/j.soscij.2014.07.002
0362-3319/

& Thong, 2013). To achieve a balance between the benefits and risks of personal information use, the Obama administration in 2012 unveiled a Consumer Privacy Bill of Rights. In the bill of rights, one of the most important principles for protecting information privacy is the *individual control principle*, by which consumers "have a right to exercise control over what personal data companies collect from them and how they use it" (The White House, 2012, p. 10). Under this principle, an ISP can use a person's personal information only after obtaining the person's consent.

Although the individual control principle might be a reasonable solution to balance information privacy and the legitimate use of personal information by ISPs, ordinary Internet users still fall victim to privacy infringement because of consent form design flaws and user carelessness. First, subtle differences in the design of consent forms have a substantial influence on the perceived importance of information privacy. Some studies (Jamal, Maier, & Sunder, 2005; Johnson, Bellman, & Lohse, 2002) show that it is easier for an ISP to obtain consent for use of personal information under an opt-out frame, a format where a user is assumed to give consent unless explicitly declining, than under an opt-in frame, a format where a user is assumed to decline unless giving explicit consent. In other words, by adopting a seemingly fair but shrewd answer format, an ISP could threaten information privacy. Second, users do not pay sufficient attention to the fine print of ISP privacy policies. For example, an experiment by McDonald and Cranor (2008) demonstrates that most people simply skim the terms of privacy policies and hastily give consent for the use of personal information. In short, carelessly giving consent may endanger information privacy.

Only two studies (Jamal et al., 2005; Johnson et al., 2002) test how differences in consent forms influence people's decisions regarding their own information privacy. Even those studies are limited, as the experiments examine only e-mail address. In fact, according to research on Social Network Service (SNS) users' privacy management (Lenhart & Madden, 2007; Rainie, Kiesler, Kang, & Madden, 2013), people pay more attention to privacy regarding certain sensitive items like social security number and physical address while exhibiting less concern about other items like views on issues or products or chats on SNS. Thus, there is between-item variance in privacy perceptions. Additionally, opinion polling finds that people with more strongly held privacy beliefs and those with prior privacy infringement experience tend to put more emphasis on information privacy (Baek, Kim, & Bae, 2014; Dinev et al., 2013; Westin, 2003). Thus, between-people variance in privacy perceptions should be investigated.

This study, therefore, examines whether the frame of consent forms influences the giving of consent, and it investigates the presence of between-item and between-people variance in the framing effect. Unlike prior studies that find a framing effect for one personal information item (Jamal et al., 2005; Johnson et al., 2002), this experiment examines an extensive range of 17 items in order to identify which items are vulnerable to the framing effect. Additionally, this study investigates how the framing effect varies depending on two personal characteristics: attitudes about information privacy and prior experience of privacy infringement. Guided by the framework of prospect theory (Kahneman, 2011; Kahneman, Knetsch, & Thaler, 1991; Kahneman & Tversky, 1979) as applied in information privacy research and the behavioral sciences, an online survey experiment was conducted with representative Korean Internet users.

2. Information privacy, consent forms, and status quo bias as a framing effect

A basic, commonly adopted method of protecting online privacy is to implement a legal mandate for an ISP to obtain user consent for use of personal information in the course of the ISP's business (The White House, 2012). Such a notice-and-consent requirement (Peppet, 2012, p. 1153) allows people to either protect their online privacy by declining consent or to knowingly accept the risk of privacy infringement by consenting to the ISP's request. In other words, with the notice-and-consent requirement, users choose between consenting and taking the risk of privacy infringement or declining and taking no risk.

How people make decisions under risk and uncertainty has been studied actively by scholars in the fields of cognitive psychology (Gilovich & Griffin, 2010), behavioral economics (Sunstein, 2013; Thaler & Sunstein, 2008), and other behavioral sciences (Druckman & Nelson, 2003; Kim, 2012; Krosnick, 1999). One of the dominant theories with regard to judgment under risk is prospect theory (Kahneman & Tversky, 1979). Given that Internet users are forced either to consent or decline under risk, prospect theory is a good theoretical framework.

One of the key arguments of prospect theory is that people tend to overweight "outcomes that are obtained with certainty," which "leads to inconsistent preferences when the same choice is presented in different forms" (Kahneman & Tversky, 1979, p. 47). This insight bears relevance to the two frames—opt-in and opt-out—that Internet consent forms use (Peppet, 2012; Schwartz, 2013; Sovern, 1999). In essence, consent forms with an opt-in frame require people to give explicit consent for an ISP to use their personal information; declining consent is the default choice. Users, in other words, must consciously accept the risk of privacy infringement under the opt-in frame. On the other hand, consent forms with an opt-out frame require people explicitly to decline consent if they wish to protect their privacy; giving consent is the default choice. In this case, users must pay additional attention to the privacy policy terms if they wish to protect their own information privacy.

According to prospect theory (Kahneman, 2011; Kahneman et al., 1991), information privacy is assessed differently in these two frames. Although the mathematically expected privacy outcomes may be logically equivalent because the probability of choosing protection is the same as that of choosing no protection, prospect theory does not treat the two frames as identical because they adopt different default information privacy choices. Under the opt-in frame, people must make an effort to give consent, but this consent leads to a loss in privacy. Under the opt-out frame, people must consciously decline to give consent, leading to a gain in information privacy. Therefore, the default state