International Journal of Information Management 38 (2018) 262–269

Contents lists available at ScienceDirect

International Journal of Information Management

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

# Untangling the relationship between surveillance concerns and acceptability

Taewoo Nam

*Department of Public Administration, Graduate School of Governance, Sungkyunkwan University, 25-2 Sungkyunkwan-ro, Jongno-gu, Seoul 03063, Republic of Korea*

ARTICLE INFO

*Keywords:*
Government monitoring
Surveillance acceptability
Surveillance concerns
Privacy concerns
Privacy control

ABSTRACT

In this study, a two-stage least squares regression analysis of data from the Pew Research Center's Privacy Panel Survey sought to untangle the relationships among surveillance concern, its antecedents, and the acceptability of surveillance as an attitudinal outcome. The analysis assumes the endogeneity of surveillance concerns, drawing from theoretical arguments. Surveillance concerns, as predicted by empirical antecedents (perception of privacy control, past negative experiences, surveillance awareness, and information sensitivity), significantly influence surveillance acceptability. Significant exogenous determinants of surveillance acceptability include perceived public benefit and self-identified ideological stance.

## 1. Introduction

Privacy concerns are critical to empirical research on information privacy. In particular, studies examining the antecedents-privacy concern-outcomes (APCO) model highlight the complex role of privacy concerns as an explanatory variable, an explained variable, or both (Smith, Dinev, & Xu, 2011). Even though a stream of research on privacy concerns has created well-articulated arguments and well-established areas of research, space still exists within this stream for addition and augmentation. This study identifies government surveillance as a form of information privacy intrusion and the endogenous treatment of privacy concerns' dual roles as a niche in the literature.

In that niche, only a few studies have dealt with information privacy concerns in the context of government surveillance (e.g., Dinev, Bellotto, Hart, Russo, & Serra, 2006; Dinev, Hart, & Mullen, 2008; Lim, Cho, & Sanchez, 2009; Pavone & Esposti, 2012; Smith, 2005), while many studies focus on concerns about information privacy intrusion by advertisers and companies. Academics validated the APCO model through structural equation modeling and multivariate analyses (Phelps, Nowak, & Ferrell, 2000), but given the dual roles of information privacy concerns, their evidence-supported endogeneity merits empirical examination through two-stage least squares (2SLS) regression analysis.

Given those two gaps in the existing research, this 2SLS-based analysis tackles the following research questions: 1) What determines concerns about government surveillance? (the first stage of the 2SLS); and 2) What determines surveillance acceptability as an outcome of government surveillance concerns? (the second stage of 2SLS). To address those inquiries, this study uses data from the Pew Research Center's Privacy Panel Survey. The remainder of this article proceeds as follows. Section 2 draws relevant conceptual constructs from a review of previous literature. Section 3 describes the measurements and method (2SLS). Section 4 reports the results of 2SLS analysis. Section 5 discusses theoretical and practical implications of the results. Section 6 concludes the paper.

## 2. Reviewing antecedents and outcomes of privacy concerns

Privacy concerns as "a measurable proxy for privacy" (Smith et al., 2011: 997) have attracted interest from information privacy researchers. Given that the measurable concept simply describes "the extent to which individuals believe they might lose their privacy" (Dinev et al., 2008: 218), its empirical role is complicated and dual: it can be a dependent variable or an independent one (Dinev & Hart, 2004; Smith et al., 2011). This duality leads to diverse findings and implications in terms of how privacy concerns can be measured, what influences privacy concerns (antecedents), and what privacy concerns influence (outcomes) (e.g., Acquisti, Brandimarte, & Loewenstein, 2015; Awad & Krishnan, 2006; Bélanger & Crossler, 2011; Culnan & Armstrong, 1999; Dinev & Hart, 2004). Some previous studies (Clarke, 1999; Dinev et al., 2006, 2008) addressed Internet privacy concerns regarding government surveillance and considered willingness to provide personal information to be an outcome of concerns. As these studies observed, government intrusion concerns in many countries adopting surveillance technologies can be considered a form of Internet privacy concern. This paper focuses on Internet privacy concerns in the context of government surveillance, examining whether the usual antecedents of privacy concerns in the APCO model can be applied to the surveillance context. It also extends the logic underlying the APCO model to the surveillance context and consideration of the endogenous nature of privacy concerns in this context (the use of 2SLS as a way to examine endogeneity). In this way, the study replaces

*E-mail addresses:* namtaewoo@skku.edu, namtaewoo@gmail.com.

http://dx.doi.org/10.1016/j.ijinfomgt.2017.10.007
Received 26 June 2017; Received in revised form 26 October 2017; Accepted 26 October 2017

privacy concerns and outcomes (reactions such as intention to disclose personal information) with surveillance concerns and surveillance acceptability.

### 2.1. Privacy, surveillance, and acceptability

Privacy can be understood as "a moral right" or "a legal right" (Clarke, 1999: 60) or more generally as "the right to be left alone" (Warren & Brandeis, 1890). Although this view remains normative, behavioral practices suggest a privacy calculus, which implies that privacy-related decision-making relies on reasoned action–personal calculations of cost (risk) and benefit (Culnan & Armstrong, 1999; Culnan & Bies, 2003; Dinev & Hart, 2006a; Klopfer & Rubenstein, 1977; Laufer & Wolfe, 1977; Phelps et al., 2000; Smith et al., 2011). For a person who prioritizes privacy as "the right to be left alone," surveillance–denoting "any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered" (Lyon, 2001: 2)–necessarily hampers privacy to a substantial extent. Both reasoned and sentimental-heuristic evaluations affect the extent to which individuals achieve the normative ideal (Acquisti et al., 2015) and are willing to disclose personal information (Chellappa & Sin, 2005), intend to transact information (Dinev & Hart, 2006b), and/or engage in information disclosure behavior (Buchanan, Paine, Joinson, & Reips, 2007). In line with this argument, individual attitudes about anti-terrorism surveillance differ with and depend on both reasoned and sentimental evaluations of national and personal security (Simone, 2009: 2). Reasoned and sentimental evaluations substantially determine the level of concern about government surveillance, which refer to "a negative belief about the proactive gathering and processing of personal information and monitoring online behavior by the government" (Dinev et al., 2008: 220).

Government surveillance is a matter for the citizenry to accept and the government to justify (Dinev et al., 2006, 2008; Simone, 2009). The communication boundary management theory posits that individuals control and set boundaries (limits) around what they are willing to share with various partners, thereby drawing a line between public information and private information (Petronio, 1991, 2010, 2013). Information-processing technologies–for example, big data analysis of personal information on social networking sites, phone call logs, and Internet of Things for counterterrorism, geospatial information exploitation, and biometrics to identify and verify human terrorist subjects by analyzing a variety of biometric signatures such as faces, irises, fingerprints, and voices (Lyon, 2003; Nye & Owens, 1996)–have become surveillance technologies, which has blurred the boundaries between public information and private information (Dinev et al., 2008: 217). Thus, attitudes about government surveillance can result from privacy boundary blurring driven by surveillance use of information-processing technologies. Acceptability of surveillance is a sort of proxy to measure the balance between government intrusion to maintain social order and privacy protection for liberties. With this logic, this study considers *surveillance acceptability* as an eventual outcome of *surveillance concerns* and other determinants.

### 2.2. What determines privacy concerns?

The thorough review that Smith et al. (2011) published on information privacy research considered privacy experiences, privacy awareness, personality differences, and demographic differences as key antecedents of privacy concerns. Exposure to or victimization by personal information abuses provoke strong concerns about information privacy (Smith, Milberg, & Burke, 1996). Because surveillance can produce side effects such as abusive utilization, unreliable data, and excessive intrusion (Etzioni, 1999), past experiences of negative effects can shape surveillance-related attitudes. This study uses past experiences of privacy intrusion in the general (related to business and social activities) context instead of specific measures representing experiences of government intrusion, thereby examining whether general experiences solidify government intrusion concerns regarding the context of government surveillance. Further research is needed to determine whether privacy intrusion experiences in the general context are potentially related to concerns about government surveillance.

**H1.** Past negative experiences related to information privacy increase surveillance concerns.

Privacy awareness reflects the extent to which an individual is informed about organizational privacy practices. Existing studies (Malhotra, Kim, & Agarwal, 2004; Phelps et al., 2000) found that being informed about those practices reduces privacy concerns. In line with this argument, unawareness of surveillance (the case in which an individual is not informed of government surveillance actions) may increase concerns regarding surveillance.

**H2.** Surveillance awareness reduces surveillance concerns.

Relevant personality differences include various aspects related to defining the private sphere. Specifically, Xu, Dinev, Smith and Hart (2011) found that *self-disposition* can determine boundary opening-closing rules and affect personal risk-control assessment. Individuals who place a high value on privacy inherently cherish their personal boundaries and exhibit greater caution surrounding surveillance than those who place a low value on privacy. The degree of privacy concerns may vary with psychological traits in regard to opening or closing oneself (Li, 2014). Moreover, concerns about privacy intrusion by government surveillance also may vary with disposition regarding privacy. Including *self-disposition* is an extensive application to identifying antecedents of citizen attitudes regarding government surveillance.

**H3.** Self-disposition as a private person increases surveillance concerns.

A different line of studies took a more extensive view on antecedents of privacy concerns than the review of Smith et al. (2011). A wide array of empirical evidence strongly supports that a sense of privacy control is key to decreasing privacy concerns (Culnan & Armstrong, 1999; Dinev & Hart, 2004; Phelps et al., 2000). According to Xu et al. (2011: 804), *privacy control* is a perceptual construct that reflects an individual's beliefs in his or her ability to manage the release and dissemination of personal information. Two constructs–*perceived information control* and *perceived value of control*–describe how privacy control influences privacy concerns. *Perceived information control* explains the extent to which people believe they have control over the environment (Skinner, 1996). Those who consider personal information control important may have a high level of privacy concerns (Awad & Krishnan, 2006). In line with this, *perceived value of control* can raise concerns regarding privacy intrusion by government surveillance. *Perceived information control* as a proxy of actual control to predict behavior (Ajzen, 2002) mirrors perceptions of the ease or difficulty of privacy control (Lee, 2008: 17–18); as such, *perceived ease of control* can also be a construct of privacy control that influences privacy concerns. Previous studies empirically connected information control and perceived ease of use in the context of technology adoption (Venkatesh, 2000; Xu & Gupta, 2009). Actual control in empirical research designates whether a person can control diverse situations or events (Connell, 1985; Weisz & Stipek, 1982). If actual control indicates the ability to use such tactics as secrecy, anonymity, and confidentiality, perceived ease of diverse control tactics would relieve privacy concerns to some extent (Phelps et al., 2000; Zwick & Dholakia, 2004). Thus, this study uses *perceived ease of control* as a basic component for actual control capability.

**H4.** The multi-dimensional constructs of privacy control influence surveillance concerns.

**H4a.** Perceived information control reduces surveillance concerns.

**H4b.** Perceived value of control increases surveillance concerns.