Perceived Privacy Breach – the Construct, the Scale, and its Antecedents

Altaf Ahmad
Information Systems, Arizona State University, Tempe, AZ, United States., altaf.ahmad@asu.edu

Peter Mykytyn
Department of Management, Southern Illinois University Carbondale, Carbondale, IL, United States., mykytyn@business.siuc.edu

Follow this and additional works at: http://aisel.aisnet.org/amcis2012

Recommended Citation
http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/21

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Perceived Privacy Breach – the Construct, the Scale, and its Antecedents

Altaf Ahmad
Arizona State University
altaf.ahmad@asu.edu

Peter P. Mykytyn
Southern Illinois University Carbondale
mykytyn@business.siuc.edu

ABSTRACT
This paper describes the development of an instrument to measure the perception of privacy breaches. Perceived Privacy Breaches are divided into three dimensions: Dispersion, Fairness and Impact. These dimensions were derived using exploratory factor analysis on data gathered from 197 subjects. The instrument was utilized as part of a model to test the focal construct’s relationships with its antecedents. A multiple regression was performed on a sample constituting 70% randomly selected cases. A cross-validation of the regression equation was performed using the remaining cases. Results indicate that the level of privacy concern an individual possesses has a positive impact on the severity of perceived privacy breaches. It was also found that personal experience of privacy invasions had a negative impact on the severity of perceived privacy breaches.

Keywords
Information privacy, privacy breaches, instrument development

1. INTRODUCTION
While technology has enabled a world of information to be available to us, it has also enabled information about us to be available to the world. Today, information about individuals can be gathered not only through solicitation but also through their use of systems such as websites, e-mail and online search. This is important in light of a desire on the part of an ever more security-conscious state to gain knowledge of people and on the part of commercial firms to possess deep, insightful knowledge about their customers.

It has, not surprisingly, raised concerns regarding individual privacy and protection from unwanted intrusions. The issue has resonated in popular consciousness in the form of increased awareness and concern (Blanton, 2006); prompting privacy laws and regulations to be suggested (Kang, 2012; Angwin & Thurm, 2010; Steel, 2010). Academia has also embraced the issue of privacy in domains as varied as philosophy (Tavani, 2007), psychology (McNall and Roch, 2007), marketing (Norberg, Horne, and Horne, 2007; Barwise and Strong, 2006; Phelps, 2000; Goodwin, 1991), and information systems (Lee, 2009; Kim, Ferrin, and Rao, 2008; Awad and Krishnan, 2006; Malhotra, Kim, and Agarwal, 2004).

As the state and corporations acquire, exchange, and trade information, privacy incidents often arise. For example, America Online released to academic researchers the search query history of its users, which lead to those search queries being archived on third-party websites (Shannon, 2006). Although individual queries did not necessarily reveal much about users, when cross-referenced they revealed much more. Separately, the US Department of Justice requested a list of search queries for an entire month from all the major search engines, a request with which most firms complied (Caterinicchia, 2006). More recently, a US court ruling asked Google to provide list of all the videos users had watched if they had watched even one owned by Viacom Corporation (BBC New, 2008).

These examples raise important questions. Do we know how concerned people are about these incidents? Do they actually regard them as breaches of privacy? If so, how severe a breach do these incidents represent? Do some privacy breaches concern people more than others? How does one compare one privacy breach to another?

These questions form the motivation for this research. More specifically, it involves the development of a new construct, Perceived Privacy Breach, to evaluate the perceived severity of a privacy breach. After having established the validity of the construct, we will utilize it in a model that investigates the antecedents of perceived privacy breaches.
The perspective that this research investigates privacy from can be distinguished from extant approaches in two ways. First, much of the privacy research in the literature is forward-looking in that it considers privacy concerns of individuals and how they might affect their behavior in the future (Phelps, 2000; Liu, Marchewka, Lu, and Yu, 2005; Dinev and Hart, 2006). In contrast, we look at the perception of events that have already occurred.

Second, studies on privacy focus largely on the experience of the person in question e.g. personal experience of privacy invasions (Awad and Krishnan, 2006). Such an approach would not take into account the effect of privacy incidents in the external environment that may not have directly impacted people themselves. The present research fills that gap.

The rest of this paper charts out the background of relevant privacy research, presents theoretical support for the construct and the proposed model, and presents the results of the study.

2. BACKGROUND

The study of privacy has been varied and spread across different disciplines. Philosophical perspectives have been applied to consider what privacy is, whether individuals have a right to it, and how individuals can be deemed to possess it (Moor, 1990, 1997). The notion of privacy has also changed as time has progressed. Whereas once it referred to the notion of freedom from intrusion or interference (Tavani, 2007), modern notions of privacy are concerned with protection of information or information privacy (Stone, Gardner, Gueutal, and McClure, 1983; Westin, 1967). Information privacy has often been conceptualized as an issue of control of information, and it is this perspective of privacy that is commonly utilized in the literature (Taylor, Davis, and Jillapalli, 2009; Awad and Krishnan, 2006; Malhotra, et al., 2004; Dinev and Hart, 2004). However, other conceptualizations regard total control as unattainable and propose that regulation or access to information is the central issue of privacy (Tavani, 2007; Moor, 1997).

Since technology users are also consumers, related privacy research occurs at a confluence of Organization Science, Marketing and MIS literatures. Research in the area of privacy concern has focused on evaluating its factors or antecedents (Dinev and Hart, 2004; Culnan, 1993), studying approaches to encouraging consumers to disclose information about them (Phelps, 2000; Andrade, Kalcheva, and Weitz, 2002), studying the effects of privacy policies (e.g., Li & Zhang, 2009) and measuring privacy concern by devising scales such as Global Information Privacy Concern and Concern for Information Privacy (Smith, Milberg, and Burke, 1996). In related MIS research, these scales were extended to the online realm in the form of the Internet Users Information Privacy Scale (IUIPC) (Malhotra, et al., 2004), which decomposes concern for privacy into concern about information collection, control and awareness of privacy-related practices.

Privacy concerns have been shown to have an effect on risk and trust beliefs (Malhotra, et al., 2004), which in turn play a significant part in individuals’ willingness to transact and provide personal information on the Internet (Kim, et al., 2008; Cazier, Wilson, and Medlin, 2007; Dinev and Hart, 2006; Liu, et al., 2005).

While there has been a focus on privacy concern in general, people’s reaction to privacy breaches has not received as much attention. Relevant research in that context includes findings that security incidents have an impact on financial performance of organizations (Acquisiti, Friedman, and Telang, 2006) and that experience of privacy invasions did not seem to have an effect on individuals’ decision to share data (Awad and Krishnan, 2006).

The theoretical underpinning of privacy research encompasses a number of different frameworks such as social contract (Malhotra, et al., 2004; Culnan and Armstrong, 1999), social exchange theory (Andrade, et al., 2002), privacy calculus (Dinev and Hart, 2006; Culnan and Armstrong, 1999) and procedural fairness (Culnan and Armstrong, 1999) to name a few. These can broadly be viewed in two strands: one that suggests that individuals will willingly provide information about themselves if they derive a benefit out of it (Andrade, et al., 2002; Culnan and Armstrong, 1999), and the other that individuals will evaluate the appropriateness of information usage by a firm based on the understanding they had with the organization (Malhotra, et al., 2004; Culnan and Armstrong, 1999).
3. RESEARCH MODEL AND HYPOTHESES

3.1 Privacy Breach

We define a Perceived Privacy Breach as an individual’s perception that an exchange of information – be it voluntary or involuntary – between two or more parties represents a breach of someone’s privacy. Such a perception can be held about any exchange of information and would not be restricted to only those exchanges that an individual is personally involved in.

As people encounter exchanges of information between commercial and/or government institutions, they might form opinions as to the exchanges’ legitimacy and fairness (Culnan and Armstrong, 1999). However, it is likely that not all potential privacy breaches will be perceived by people as being of the same severity. For example, providing mailing addresses of customers by one firm to another is likely to be regarded differently than a public disclosure of credit card numbers. Providing electronic records to the government would be perceived differently based on whether a firm was under a subpoena or not. Likewise, the release of medical records to an insurance company will probably be interpreted differently than if they were to be released to one’s neighbors.

We can surmise from these examples that privacy breaches would be evaluated along several areas of concern. We expect that these would include the nature of the information, the risk that people were exposed to as a result of that exchange, and to whom the information was released. The concerns for privacy that people have would also be reflected in how they perceive privacy breaches. Accordingly, control of information, secondary use, and perception of procedural fairness would be probable factors in determining the perceived severity of a privacy breach. The aforementioned factors would combine with an evaluation of the magnitude of the breach (e.g., how many people had access to the leaked information, if it was released on the Internet, etc.) to form the dimensions of the Perceived Privacy Breach construct.

3.2 Hypotheses

Those individuals who are more concerned about their privacy can also be expected to place a high degree of value on it. By placing a high degree of value on privacy and by being concerned about it, such people might be more sensitive to its violation. Concern for privacy would manifest in many ways. It has been shown to affect beliefs regarding risk and trust in firms to protect their information (Malhotra, et al., 2004). Privacy breaches will also be intricately tied to beliefs about trust and risks as they will be indicators of the risks people are exposed to. Just as increased privacy concern tends to affect beliefs about risk (Malhotra, et al., 2004), we argue that they will also affect beliefs about how severe privacy breaches in the environment may be. Those people who are more concerned about privacy issues can be expected to take a sterner stand against privacy breaches and regard them as more severe than those who are not as concerned about privacy. Accordingly, we hypothesize the following.

\[ H1: \text{Privacy concern will have a positive relationship with the severity of perceived privacy breaches.} \]

We consider next how experience of privacy breaches might affect the way people might perceive their future occurrence. It is plausible that prior experience of privacy breaches or invasions would have an effect on people’s perceptions as knowledge of the past helps make low probability events more salient (Ajzen and Fishbein, 1980), shapes future intentions, and models
behavior (Fishbein and Ajzen, 1975). Having knowledge of privacy breaches would make prominent to people the risks associated with having information about themselves compromised.

Therefore, it can be expected that if people perceive themselves as having been victims of privacy invasions – even if that perception was incorrect – they might be more wary of privacy risks and consequently attribute more weight to future privacy breaches. The more frequent the perceived invasions, the more severe they might regard future privacy breaches.

\[ H2: \text{The perceived frequency of privacy invasions experienced will have a positive relationship with the severity of perceived privacy breaches.} \]

Further, we consider if knowledge of privacy breaches to others might have an effect on how people perceive future occurrences. Since a person’s behavior is shaped by his or her interaction with the environment (Bandura, 1977; 1986), the experience of encountering privacy breaches in the external environment would probably also affect how they think and behave in relation to evaluating perceived privacy breaches.

In addition to having knowledge about their own experiences, people also absorb information from their environment. If a personal acquaintance suffers some form of privacy invasion, it is likely that that will be factored into account by people as they evaluate their risks. Accordingly, knowledge of past violations of privacy to acquaintances (friends or family) would have an effect on how people evaluate privacy breaches. The more the perceived violations, the more weight one would attribute to them. However, privacy invasions suffered by acquaintances will probably have a lesser degree of effect on a person than privacy invasions suffered by the person itself.

\[ H3: \text{The perceived frequency of privacy invasions experienced by acquaintances will have a positive relationship with the severity of perceived privacy breaches.} \]

4. METHODOLOGY

4.1 Instrument Development and Validation

A new instrument was developed to measure Perceived Privacy Breaches (PPB). With the expectation that some privacy concerns will be reflected in how people judge privacy breaches, items were drawn partly from extant literature that showed concern about control, risks and sensitive information. Items related to information access were also created in view of the access-oriented view of privacy (Tavani, 2007; Moor, 1997). A scenario of a privacy breach to be used in conjunction with the questionnaire was created with the help of judges. The instrument was pre-tested with a small sample for face validity and clarity.

The research utilized 197 student participants from a large university. Study participants were asked to read the scenario about a privacy breach and for each item indicate on a 5-point Likert-like scale whether they agreed with that item. Each item denoted a possible reason as to why the scenario represented a severe breach of privacy.

Exploratory Factor Analysis was conducted using Varimax rotation in SPSS 15 to extract the latent dimensions of privacy breaches and to reduce items. An analysis of internal consistency was carried out for the factors to ensure reliability. The result was a 3 factor solution with the dimensions representing dispersion of information (α = .80), fairness (α = .79), and potential impact of the breach (α = .74), all of which had satisfactory alpha levels of over .70 (Hair, Black, Babin, Anderson, and Tatham, 2006). Scale means were 18.08 (SD = 3.14) for dispersion, 19.38 (SD = 3.33) for fairness, and 13.62 (SD = 2.78) for impact. Items for the individual scales can be found in Table 2 in the appendix.

4.2 Other Measures

Perceived frequency of privacy invasions to self (FQP) and acquaintances (FQA) were measured using a single item question that asked participants to rank how frequently they felt they had suffered an invasion of privacy. This allowed for knowledge of past privacy invasions as well as their perceived frequency to be accounted for. Acquaintances were defined as “family and friends.” The ranking was along a 5-point Likert-like scale from “very infrequently” to “very frequently.” Information privacy concerns were measured using the IUIPC instrument (Malhotra, et al., 2004). The IUIPC instrument was measured along a 5-point scale to maintain consistency with the rest of the research instrument. Subscale scores from the three dimensions of IUIPC were averaged to form a composite interval score. The questionnaire items can be found in the appendix.
4.3 Analysis
The sample of 197 observations was split, at random, into two samples representing approximately 70 percent of the cases (sample A) and 30 percent of the cases (sample B). Such data splitting has been described as being an acceptable way of model validation (Snee, 1977). Sample A was used to perform a standard multiple regression analysis in SPSS 15 using PPB as the criterion variable and privacy concerns (PC) and the two frequency variables (FQP and FQA) as the predictor variables. Refer to the appendix for descriptive statistics of sample A. Cases with missing data were excluded list-wise. Sample B was used as hold-out sample for cross-validation.

In order to perform the cross-validation, the regression equation from sample A was used to calculate composite predicted criterion scores in sample B. The expectation was that if the regression equation we derived from sample A was a good model of the data, then there would be a high degree of correlation between the predicted and actual criterion scores for the hold-out sample B. If the resulting $R^2$ value was comparable to the $R^2$ value of the regression model, then the model would be supported (Osborne, 2000). Accordingly the predicted criterion scores for sample B were correlated with the actual criterion scores of sample B and $R^2$ values calculated.

5. RESULTS

<table>
<thead>
<tr>
<th>Coeff</th>
<th>Intercept</th>
<th>IUIPC</th>
<th>FQP</th>
<th>FQA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ustd</td>
<td>9.741</td>
<td>.592</td>
<td>-.594</td>
<td>.294</td>
</tr>
<tr>
<td>Std</td>
<td>.479</td>
<td>-2.37</td>
<td>.124</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Coefficients from the standard multiple regression (n = 123)

Regression analysis revealed that the model significantly predicted the severity of perceived privacy breaches, $F (3, 119) = 12.27, p < .0001$. $R^2$ for the model was .236, and adjusted $R^2$ was .217. Table 1 displays the unstandardized coefficients (B), intercept, and standardized regression coefficients ($\beta$) for each variable.

In terms of individual relationships between the predictor and criterion variables, privacy concern ($t = 5.81, p < .0001$) and frequency of privacy invasion experiences ($t = -2.21, p < .024$) each significantly predicted the severity of perceived privacy breaches. However, the frequency of privacy invasions to acquaintances was not statistically significant ($t = 1.16, p < .25$). The following regression equation was obtained: $\hat{Y} = 9.741 + (.592 \times \text{Privacy}) - (.594 \times \text{Frequency of privacy invasions to self}) + (.294 \times \text{Frequency of privacy invasions to acquaintances})$.

The first hypothesis that privacy concerns would have a positive relationship with the severity of privacy breaches was supported ($p < .0001$). The second hypothesis that the frequency of having experienced privacy invasions would have a positive relationship with the severity of privacy breaches was statistically significant but in the opposite direction ($p < .024$). The third hypothesis was not supported ($p < .25$).

The cross-validation returned acceptable results. The correlation of the predicted criterion scores with actual criterion scores of the hold-out sample B was .453 ($R^2 = .205, n = 62$) where the $R^2$ of the original model was .236. Since there is a small difference (3%) in the degree of explained variance, there is support for the regression model that was yielded by this analysis.

6. DISCUSSION
This paper has started conceptual development of evaluating privacy breaches from the third person perspective. It has been different from extant approaches in that it looks at privacy breaches that might not have directly impacted a person.

We also tested a model to determine how privacy concerns and perceived privacy invasions – those experienced personally and contacts – would affect people’s judgment of privacy breaches.

H1 was supported as expected. Privacy concerns and evaluation of privacy breaches show a moderate degree of correlation ($r = .465$). This establishes, first, that people who are more wary about privacy are also likely to perceive privacy breaches as
more severe. Second, the lack of a very high degree of correlation between privacy concern and perceived privacy breaches supports the argument that these two constructs while related are not interchangeable.

The finding that perceived frequency of personal privacy invasions had a negative relationship with severity of perceived privacy breaches was surprising. The standardized beta suggests that for every standard deviation increase in frequency of personal invasions, the severity of perceived privacy breaches decreases by .24 standard deviations holding all other predictors constant. This result is counter-intuitive as one would expect that experience of privacy breaches would tend to make people more wary and perceive future breaches as more suspect or severe. Nevertheless, there seems to be some consistency with Awad and Krishnan’s (2006) finding which suggested that experience of privacy invasions did not deter people from sharing information about themselves. The present result can possibly be understood as such: the more people suffer what they think is an invasion of their privacy, the more they are used to it and tend to view future privacy breaches as less severe. This could possibly be attributed to people finding that not all privacy breaches are very severe and have a great impact on their lives. They might be more circumspect in considering what may or may not affect people. Alternatively, the nature of the privacy breach that people have been exposed to might also have an effect. Further research needs to be conducted in this regard to resolve this issue.

The finding that knowledge of privacy invasions of acquaintances does not have an effect on individuals’ ranking of privacy breaches suggests that individuals may not consider others’ breaches as being relevant to their own experience and act largely on the basis of their experience alone.

7. LIMITATIONS

How privacy breaches are perceived may be subject to one’s experiences in life. The use of students imposes the limitation that their concerns for privacy might not be sufficiently developed. The concerns of younger people might also be different than those of older ones. Questions of generalizability thus arise.

Other methodological concerns that we have to acknowledge pertain to the limitations of survey-based research in general. We have based our study on one questionnaire that collected data about both the independent and the dependent variables. This exposes the study to common method variance, as certain respondents might consciously or unconsciously report answers to dependent variables that are consistent with what they have reported for independent variables.

There are also some concerns about using data derived from Likert scales in techniques that require interval data. While we have used such data, there is also some support that regression is robust enough to withstand the use of ordinal data in that Type I and Type II errors are not affected dramatically (Jaccard and Wan, 1996).

8. FUTURE DIRECTIONS

In creating an instrument to measure privacy breaches, this research has created room for raising other appealing questions. First, it allows for the evaluation of people’s perception of privacy breaches that are well-publicized and to consider whether people actually consider popularly known privacy breaches as being severe. Second, that information can be then be utilized to answer other questions. Is people’s concern for privacy heightened as a result? Would people’s behavior change as a result of being cognizant of privacy breaches? We hope to address some of these questions in the near future.

9. REFERENCES


10. APPENDIX

Perceived Privacy Breaches: Items to be rated on a 5-point Likert-like scale from Strongly Disagree to Strongly Agree. Items should be customized with the people affected by privacy breaches.

<table>
<thead>
<tr>
<th>Displacement</th>
<th>The information was released to a lot of people.</th>
</tr>
</thead>
<tbody>
<tr>
<td>α = .80</td>
<td>The information was released to people in different jurisdictions, states or countries.</td>
</tr>
<tr>
<td>M=18.08</td>
<td>The information released was not restricted to a small set of people.</td>
</tr>
<tr>
<td>SD= 3.14</td>
<td>Too many people could have access to that information now.</td>
</tr>
<tr>
<td></td>
<td>Information was released over a wide geographical area.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fairness</th>
<th>Unauthorized persons had access to the information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>α = .79</td>
<td>It was unfair for the information to be given out.</td>
</tr>
<tr>
<td>M=19.38</td>
<td>It was wrong for the information to be released.</td>
</tr>
<tr>
<td>SD= 3.33</td>
<td>Only the right people had access to the information.*</td>
</tr>
<tr>
<td></td>
<td>The people who obtained access to the information could be trusted.*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact</th>
<th>Information released could potentially identify John as breaking laws.</th>
</tr>
</thead>
<tbody>
<tr>
<td>α = .74</td>
<td>Information released could potentially cause John problems in the family problems at the workplace.</td>
</tr>
<tr>
<td>M=13.62</td>
<td>Information released could potentially cause loss in John's professional reputation.</td>
</tr>
<tr>
<td>SD= 2.78</td>
<td>Information released could potentially cause John problems at the workplace.</td>
</tr>
</tbody>
</table>

* Reverse-coded Items

Table 2. Perceived privacy breaches

Frequency of personal privacy invasions: How frequently have you personally been the victim of what you felt was an improper invasion of privacy?

Frequency of privacy invasions to acquaintances: How frequently have your family and friends personally been the victim of what you felt was an improper invasion of privacy?

Information Privacy Concern (from [10]): Control: (1) Consumer online privacy is really a matter of consumers’ right to exercise control and autonomy over decisions about how their information is collected, used, and shared. (2) Consumer control of personal information lies at the heart of consumer privacy. (3) I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

Awareness: (1) Companies seeking information online should disclose the way the data are collected, processed, and used. (2) A good consumer online privacy policy should have a clear and conspicuous disclosure. (3) It is very important to me that I am aware and knowledgeable about how my personal information will be used.

Collection: (1) It usually bothers me when online companies ask me for personal information. (2) When online companies ask me for personal information, I sometimes think twice before providing it. (3) It bothers me to give personal information to so many online companies. (4) I’m concerned that online companies are collecting too much personal information about me.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Mean</th>
<th>SD</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPB</td>
<td>16.88</td>
<td>2.23</td>
<td>123</td>
</tr>
<tr>
<td>IUPC</td>
<td>13.12</td>
<td>1.80</td>
<td>123</td>
</tr>
<tr>
<td>FQP</td>
<td>2.37</td>
<td>.89</td>
<td>123</td>
</tr>
<tr>
<td>FQA</td>
<td>2.66</td>
<td>.94</td>
<td>123</td>
</tr>
</tbody>
</table>

Table 3. Descriptive Statistics (sample A)