*Article*

JIS

Journal of Information Science
2017, Vol. 43(5) 583–600

DOI: 10.1177/0165551516653590
journals.sagepub.com/home/jis
SAGE

# An empirical test of an Antecedents – Privacy Concerns – Outcomes model

**John H. Benamati**
Miami University, Ohio, USA

**Zafer D. Ozdemir**
Miami University, Ohio, USA

**H. Jeff Smith**
Miami University, Ohio, USA

**Abstract**
This study extends privacy concerns research by providing a test of a model inspired by the 'Antecedents – Privacy Concerns – Outcomes' (APCO) framework. Focusing at the individual level of analysis, the study examines the influences of privacy awareness (PA) and demographic variables (age, gender) on concern for information privacy (CFIP). It also considers CFIP's relationship to privacy-protecting behaviours and incorporates trust and risk into the model. These relationships are tested in a specific, Facebook-related context. Results strongly support the overall model. PA and gender are important explanators for CFIP, which in turn explains privacy-protecting behaviours. We also find that perceived risk affects trust, which in turn affects behaviours in the studied context. The results yield several recommendations for future research as well as some implications for management.

**Keywords**
information privacy; risk, trust

## 1. Introduction

Information privacy is of growing concern to multiple stakeholders including business leaders, privacy activists, scholars, government regulators and individual consumers [1]. Surveys indicate mounting concern among Internet users and confirm privacy as a top priority for businesses. For instance, a Consumer Reports poll revealed in 2008 that 72% of consumers were concerned that their online behaviours were being tracked and profiled by companies [2]. This number has recently reached 92% in the UK, where 33% of Internet users are more concerned about their online privacy now than a year ago. These concerns are warranted in general, because not only are consumers' online behaviours tracked, but most websites also use personal information for customised advertising, and a large number of firms like Google, Yahoo, Microsoft and Facebook share their collected customer data with hundreds of their affiliated companies [3]. Such extensive use and sharing of consumer data brings with it the risk of data breach and the corresponding negative psychological impacts on consumers. Consequently, consumers must carefully weigh each of their disclosure decisions and guard against the use and sharing of their personal information without consent [4].

While growing concerns about information privacy have been noted worldwide since the 1970s, the majority of privacy-related research articles have been published since the mid-1990s. Recently, some rigorous attempts to provide an over-arching framework that explains this research stream have been undertaken. In the May 2011 issue of *Communications of the Association for Information Systems*, Li [5] reviewed a number of studies in the e-commerce domain and focused on individual-level privacy concerns (general and specific), antecedents to those concerns and

**Corresponding author:**
John 'Skip' Benamati, Department of Information Systems and Analytics, Farmer School of Business, Miami University, Oxford, OH 45056, USA.
Email: benamajh@miamioh.edu

**Table 1.** Empirical studies in information privacy research.

| Antecedents ⇒ Privacy Concerns | Privacy Concerns ⇒ Outcomes | Antecedents ⇒ Privacy Concerns ⇒ Outcomes |
|---|---|---|
| [9–23] | [24–44] | [45–49] |

Studies published prior to 2008 were identified in the database prepared by Smith, Dinev and Xu for their 2011 article in the 'Theory and Review' section of *MIS Quarterly* [7], and we gratefully acknowledge those authors for allowing us to use their database. Studies published from 2008 to date were located via searches in the ISI Web of Science, using 'privacy concerns' as a keyword. In total, 209 articles were found, and the entire text of each such article was examined. Although we cannot claim that this algorithm resulted in an exhaustive set, it is likely to have identified the vast majority of salient studies.

consequences of those concerns. In December 2011, *MIS Quarterly* published two 'Theory and Review' papers directed towards information privacy [6, 7] and the same issue included a reflection on the two 'Theory and Review' papers by Pavlou [8]. Bélanger and Crossler [6] noted especially the need for multi-level studies and for studies that focus on 'design and action', which would '[s]pecifically design a tool for providing information privacy or a framework to evaluate such tools' [6, p. 1023].

Smith et al. [7] demonstrated that almost all of the positivist empirical assessments of privacy could be viewed within a macro framework they called 'Antecedents – Privacy Concerns – Outcomes' (APCO). They noted that the majority of existing research has been focused on approximations to the latter portion of this model: examinations of the relationships between privacy concerns and different outcomes associated with those concerns, such as regulation preferences and stated intentions regarding information disclosure behaviours. They highlighted the fact that only a few studies have considered actual behaviours; most have focused on stated intentions. Further, they noted that the former portion of the model, which focuses on antecedents to privacy concerns – such as privacy experiences, privacy awareness (PA), demographic differences and others – and their relationships with privacy concerns, has received proportionately less attention. Our own recent review of literature confirms these observations, as illustrated in Table 1.

The first column in Table 1 lists studies that have a construct for privacy concerns in their model as a dependent variable [9–23], while the second column documents studies that have privacy concerns as an independent variable leading to one or more behavioural outcomes (e.g. intention to disclose personal information) [24–44]. Studies that look across the entire APCO framework by incorporating antecedents of privacy concerns, privacy concerns as well as behavioural outcomes (noted in the third column) form a very limited set of only five studies.

Note that one additional combination of selected constructs could conceivably exist: a test of antecedents and their relationship to outcomes without an intermediate measurement of privacy concerns. However, from the perspective of privacy research, such a group of studies appears to constitute a null set, likely because such papers would not generally be labelled 'privacy' studies in the IS domain. Even if they were labelled as such, they would no doubt suffer from statistical 'omitted variable bias', assuming the correctness of the arguments of Li [5] and Smith et al. [7].

Therefore, we hold that the most instructive studies in this domain are those that consider at least some variables from each of the domains on the full path from antecedents through privacy concerns and outcomes. Such studies will not only provide information systems researchers a fuller view of the issues involved, but they will also address a neglected area in the privacy literature. It is in this domain – the third column of Table 1 [45–49] – that the present study is situated. As can be seen in Table 2 (fourth column), four of the five existing studies that look across the entire APCO framework by incorporating antecedents of privacy concerns, privacy concerns and behavioural outcomes embrace a measure of 'privacy concerns' that differs somewhat from that defined in the instrumentation efforts in IS [18, 33, 50], subsequently confirmed in the literature and utilised in this study. In addition, most of the studies in the third column of Table 1 rely either on student samples (see [51] for a discussion of the appropriateness of such samples) or on what appear to be convenience samples (e.g. high-tech company employees merged with EMBA students). Only one of the five studies [49] utilises a sample drawn from a broad population via a professional research firm, the approach that is taken in this study. In addition, as can be seen in the final column of Table 2, none of the five studies uses a multi-item dependent variable scale that measures subjects' behaviours in a real-world context, as we do in this study.

It appears, therefore, that this study is the first that simultaneously: (1) considers some variables from each of the domains on the full path from antecedents through privacy concerns and outcomes; (2) measures the construct of 'privacy concerns' as it was originally conceptualised and subsequently confirmed in the literature; (3) uses a sample drawn from a broad population via a professional research firm; and (4) measures a dependent variable associated with subjects' behaviours in a real-world context using a multi-item scale.

**Table 2.** A→PC→O studies.

| Study | Sample | Antecedents | Type of PC | DV |
|---|---|---|---|---|
| [47] | Various – convenience | Internet literacy<br>Social awareness | Information abuse[a] | Intention to transact |
| [49] | Mobile phone users (via professional research firm) | Prior negative experience | Mobile (adapted from Internet PC) | Regulatory preference |
| [45] | Students | Perceived health info sensitivity<br>Previous online privacy invasion | Health info[a] | Intention to disclose info |
| [46] | Various – some students | Internet literacy<br>Social awareness | Information abuse[a] | Intention to transact<br>Intention to retrieve privileged info |
| [48] | Students | Self-efficacy<br>Perceived severity<br>Perceived vulnerability<br>Response efficacy<br>Reward | Information abuse[a] | Privacy measure use (binary) |

[a]Called 'Privacy Concerns' (or 'Privacy Concerns for Information Abuse') in these cited articles, the items in this measurement instrument are more closely related to the construct of perceived risk as conceptualised in this study.

### *1.1. Research questions*

The APCO framework was presented by Smith et al. [7] as a composite explanation of a myriad set of findings from numerous authors. To date, few researchers have attempted a test, within one study, of a set of antecedents that might impact privacy concerns, coupled with one or more behavioural outcomes (either observed or self-reported) that may flow from the concerns themselves. In addition, most researchers who have studied outcomes have settled for self-reported intentions as their ultimate dependent variable. (It has been rare for considerations of outcomes to include tests of actual behaviours.) In the first of our four research questions, we attempt to confront the legitimacy of the APCO framework itself:

> Research Question 1: To what extent does the APCO framework provide an adequate nomological representation of the relationships associated with Concerns for Information Privacy (CFIP)?

Although it is not possible, due to the large number of constructs, to completely test the APCO framework in any single study, we attempt to drill down within the framework. We first consider the relationship between some of the most salient antecedents and privacy concerns. As was noted by Xu et al. [52, p. 800], most researchers have focused on the right-hand portion of the APCO framework (the relationship between privacy concerns and outcomes) and 'have treated the construct of privacy concerns as an antecedent to various behavior-related variables', which can be verified by comparing the size of the lists in the columns of Table 1. Although our study does include a test of the right-hand portion of the model, we provide a more exhaustive test of the model by also considering 'how individual privacy concerns can be shaped' [52, p. 800] by antecedents. Specifically, we consider how individuals' PA, formed by both their exposure to privacy-related subjects in the media and previous privacy-invading experiences, may impact their levels of privacy concern. In an early privacy study, Smith et al. [18] provided elementary tests (using single measurement items) of two similar constructs' relationships with privacy concerns, but subsequent research has not tested these relationships with either validated measures or in a larger path model. This leads to our second research question:

> Research Question 2: What is the relationship between PA and CFIP?

As Smith et al. [7] noted, trust has been consistently viewed by privacy researchers as having an important role in the privacy concerns nomological network [29, 34, 53–55], although its role within the model is inconsistently modelled. Risk, on the other hand, has seldom been considered as an explanatory construct within the studies that focus directly on the relationship between privacy concerns and outcomes; its consideration has usually been relegated to the rubric of privacy calculus, which has not previously been well integrated into the overall privacy research stream [7]. So, in this study, we consider this third research question:

Research Question 3: What are the roles of trust and risk in the APCO framework?

Smith et al. [7] refer to the disclosure of personal information as an important outcome variable and Li [5] also notes the related behaviour of protecting information. Thus, to complete our investigation of the path from factors that influence privacy concerns through self-reported behavioural outcomes, we consider Research Question 4:

Research Question 4: What is the relationship between CFIP and privacy-protecting behaviours?

To answer the above research questions, we proposed a model inspired by the APCO framework. We developed a survey through a series of data collection efforts using student samples. Whenever possible, we used previously developed and validated instruments, but new measures were developed for some constructs. The survey was administered through the online provider Qualtrics to test our hypotheses. We confirmed the measurement model and analysed the data using Partial Least Squares (PLS).

This paper makes three contributions to the extant literature. First, it provides a test of the relationships between some constructs from each of the components of the APCO framework using a non-student sample provided by a professional research firm and measuring reported behaviours (rather than intentions). Thus, it provides some empirical support for APCO's legitimacy. Second, it demonstrates the importance of PA formed from media privacy awareness (MPA) and personal privacy experiences (PPE) in explaining individuals' privacy concerns. Third, it shows that risk, which had previously been considered within the stream of privacy calculus research but seldom within the studies that make up the bulk of the privacy concerns stream, has an influential role in the relationships between privacy concerns, trust and outcomes.

The paper proceeds as follows. In the next section, we describe our research model and hypotheses. In the following section, we discuss the method for our study. We then describe our analysis and results. In the last section, we discuss our findings and how they contribute to the research stream, and we also provide suggestions for executives' actions.

## 2. Model and hypotheses

As can be seen in Figure 1, our research model includes several constructs inspired by the APCO framework: CFIP, PA, demographics (age, gender) trust, risk and behaviours.

### *2.1. Underlying dimensions of CFIP*

CFIP serves as the central construct in our model. We model CFIP as a second order construct. Although not all authors have embraced the same dimensions (e.g. see Sheehan [56]), CFIP was originally presented by Smith et al. [18] as having four unitary dimensions, which were sometimes simply averaged by early privacy researchers to form an overall score for a subject. As originally defined by Smith et al. [18, p. 172], the four dimensions are:

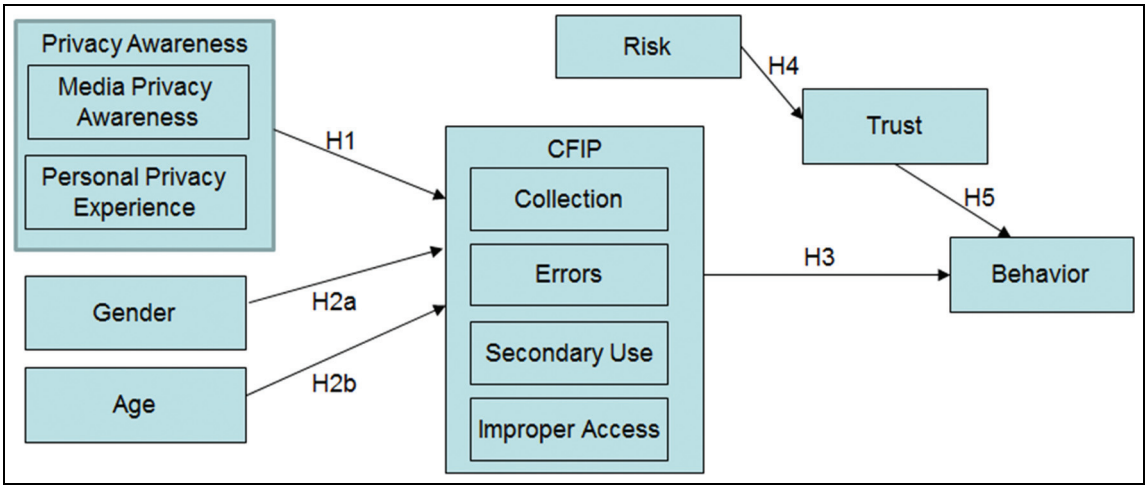


**Figure 1.** Research model.

- Collection: concern that extensive amounts of personally identifiable data are being collected and stored in databases.
- Errors: concern that protections against deliberate and accidental errors in personal data are inadequate.
- Secondary use: concern that information is collected from individuals for one purpose but is used for another, secondary purpose without authorisation from the individuals.
- Improper access: concern that data about individuals are readily available to people not properly authorised to view or work with this data.
- Although these four dimensions – and the items measuring them – have proven to have remarkable validity over time, researchers' approach to measuring CFIP has moved largely from viewing the four dimensions as unitary ones (with occasional simple averaging) to viewing them as four reflective sub-dimensions of a second-order CFIP construct. Indeed, Stewart and Segars [50] demonstrated the improved validity of such a second-order construct.

As was noted by Pavlou and Fygenson [57, pp. 119–120], 'reflective structures assume that the latent second order construct *causes* (italics in original) the first order factors…' This is the assumption upon which most recent research studies have relied: CFIP is an overriding second-order construct that causes levels of concern within the first-order dimensions of collection, errors, secondary use and improper access. Consistent with recent research, we embrace this approach in this study.

## 2.2. Antecedent: privacy awareness

Although not denoted as such, the concept of PA was first considered by Westin [58], who noted that individuals' levels of privacy concern may increase with awareness from their exposure to privacy-related media coverage and by Culnan [12] and Stone and Stone [59], who argued that this awareness may also include one's previous personal experiences. Smith et al. [18] confirmed this relationship in a rudimentary sense during their efforts to establish nomological validity of their CFIP measurement instrument. Some later research [33, 60] considered the construct of 'privacy awareness' in a different context, but the original construct has never been considered as an antecedent within a test of a robust model.

In general, individuals who have become aware of privacy-related topics – either through their own experiences or by learning of such topics through the media – can be expected to exhibit such awareness through their CFIP. Since almost all media reporting on privacy issues is focused on threats to individual privacy, and since privacy-related experiences that become salient for individuals will be primarily of a negative valence, it is likely that increased levels of PA will manifest themselves in higher CFIP. We therefore hypothesise:

**H1**: Higher levels of PA will be associated with higher CFIP.

*2.2.1. Underlying dimensions of privacy awareness.* Our argument (above), based on previous research [12, 58, 59], posited that individuals' PA is formed by their exposure to their MPA and their PPE. It is apparent, then, that PA is a second-order constructed formed by these two different dimensions.

As noted by Pavlou and Fygenson [57, p. 120], 'formative structures assume that the second-order construct is caused by the first order factors'. They further note that the dynamic nature of first-order factors is a salient consideration in determining whether a second-order construct is reflective or formative – that is, dynamic concepts 'are likely to change over time and be manipulated differently by other factors'. It is obvious that PA (the second-order construct) does not cause MPA or PPE. Thus, PA is modelled in this study as a formative second-order construct with MPA and PPE as its first order factors.

## 2.3. Antecedents: demographics

The recent review articles discussed above [5–7] all include demographics as antecedents to privacy concerns, but theoretical justification for demographic differences has been given little attention in the literature. We include hypotheses for two demographic variables that have been shown frequently to be associated with differences in privacy concerns: age and gender [11, 61–64].

*2.3.1. Age.* Researchers (e.g. [26]) frequently cite four important public opinion surveys [65–68] and responses to the benchmark question: 'How concerned are you about threats to your personal privacy in America today?[1] Are you very

concerned, somewhat concerned, not very concerned, or not concerned at all?' These surveys revealed a consistent pattern: beginning with the age bracket 18–24 years and moving upward to the age bracket 50–64 years, the percentage of respondents who answered 'very concerned' increased almost uniformly with age.[2]

By way of explanation, Regan et al. [69] argue that trends over several generations should be visible in Americans' reported privacy concerns. Of the Americans who are now most active professionally and economically (those aged younger than 70 years), concerns about privacy are likely highest in the group of 'Baby Boomers' (generally considered the group born between 1946 and 1964), who came of age during a time of cultural change and questioning of authority. Those born between 1965 and 1980 ('Generation X') came of age during a period in which trust in organisations was higher, and there was little social and political unrest. Those born since 1980 ('Millennial' generation) have grown up with technology and are therefore expected to be less concerned about privacy than their elders. Over time, this may change, as there is some evidence that teens and younger adults are becoming more alert to online dangers [69, p. 83], and a recent survey suggests that, while younger adults do exhibit lower levels of concern and engage in fewer privacy-protecting behaviours in certain areas, these differences are not stark ones [62]. However, in a cross-sectional (rather than a temporal) sense, the general expectation regarding age differences should hold as follows:

**H2a**: Increasing age will be associated with increasing levels of privacy concern.

*2.3.2. Gender.* Gender disparities have long been observed in public opinion data regarding information privacy concerns [26, 69]. Indeed, the percentage of 'very concerned' differences between male and female respondents to the Equifax, Inc. opinion surveys [66–68] shows a consistent pattern: 1990, 39% to 52%; 1993, 44% to 55%; and 1995, 41% to 52%. The same phenomenon has been found to hold in recent research studies [11, 34, 48, 53].

As with the demographic variable of age, however, only limited attention has been devoted to understanding the drivers for these differences. Two notable exceptions are studies by Metzger [63] and Sheehan [64]. Metzger [64, p. 9] notes that '[d]ifferences may be due to variations in how men and women are socialised, sex-role expectations, or in how men and women use different criteria in defining and controlling private information'. To that latter point, Sheehan [64, p. 26] cites research showing that 'women's communication consistently is involved with maintenance of social and emotional group process roles, and men consistently perform task-oriented roles'. Although not explored specifically by Sheehan, this distinction may result in men and women exchanging different types of information online, with women sharing information that they perceive to be more personally sensitive. In any event, gender-based differences in acculturation, which manifest themselves in different uses of online resources, may explain the commonly observed differences in men's and women's perspectives on privacy. Consistent with both early findings and these theoretical arguments, we posit:

**H2b**: Women will exhibit higher levels of privacy concern than will men.

## 2.4. Behaviour

As noted earlier, recent reviews of privacy research [5, 7] focus on individuals' behaviours as the ultimate reflection of their CFIP. As can be observed in the centre and third columns of column of Table 1, many studies have considered this linkage, with the majority finding expected relationships between CFIP and privacy-protecting behaviours, which often include limiting the disclosure of personal information. We expect similar findings in this study, so we hypothesise:

**H3**: Higher CFIP will be associated with privacy-protecting behaviours.

## 2.5. Trust and risk

This study defines trust consistently with Mayer et al. [70] as a willingness to be vulnerable to the actions of another. Risk is defined as 'the possibility of a loss' [71, p. 4]. The relationship between trust and risk is elusive and contextual. 'Trust is not taking risk per se, but rather it is a willingness to take risk' [70, p. 712] and be vulnerable to another party. Actually being vulnerable by taking action involves taking risk.

The roles of trust and risk in information privacy-protecting behaviours are unclear. Although the relationship between trust and privacy-related behaviours has been examined in a number of previous studies, there has not been a clear conclusion regarding trust's role. As expressed by Pavlou [8, p. 983]: '…different studies offer somewhat contradictory results regarding the exact relationship and relative effects of trust and information privacy…[T]here is a need for future

research to test the … effect of trust relative to information privacy…' Likewise, to the extent that risk has been considered in privacy-related studies, there has not been a consistent conclusion regarding risk's role in information privacy research frameworks such as APCO [14, 33, 45, 55, 72].

Dinev and Hart [72] found that risks associated with opportunistic behaviour related to the personal information collected by Internet sites negatively influence individuals' willingness to disclose personal information (trust) required to perform Internet transactions. (The study did not consider outcomes that may have resulted from this willingness/trust.) A more recent study [45] extended the work of Dinev and Hart [72] and showed that higher risk lowers willingness to be vulnerable. That study found that the general perception of risk of disclosing personal health information online has a strong negative influence on trust in a specific health website and that higher levels of trust positively influence intentions to disclose information to the health website.

We propose combining the findings from these two studies [45, 72] and hypothesise:

**H4**: Higher expressed perceptions of information-related risk when dealing with certain companies/organisations will be associated with lower trust in those companies/organisations.

Acting on a willingness to be vulnerable requires actually taking risk [70]. An alternative to simply assuming the risk in situations of low trust – where willingness to be vulnerable is low – would be to take actions to avoid the risk. In the case of information privacy-related risk, this would suggest an increase in privacy-protecting behaviours. Individuals might limit the amount or type of information that they share or limit access to that information to the extent possible. This suggests that an inverse relationship exists between trust and privacy-protecting behaviours. Hence, we hypothesise:

**H5**: Higher information-related trust in certain companies/organisations will be associated with fewer privacy-protecting behaviours when dealing with those companies/organisations.

## 3. Method

A survey was developed and measurements were validated through a series of data collections using student samples. We then implemented the survey online, using a general (non-student) sample to test the hypotheses. The following subsections provide the details of the measurement development and implementation.

### *3.1. Measures*

Whenever possible, we used previously developed and validated instruments as the basis for measuring the constructs of interest in this study. All items used a 1 to 5 Likert scale (see Appendix A for a list of all measurement items and scales). Because of the potential sensitivity of some items, the survey included the preamble: 'So that you can describe yourself in an honest manner, your responses are completely anonymous and cannot be associated with you'.

The items associated with MPA and PPE were developed by this study's authors, inspired by the single-item measures employed by Smith et al. [18].[3] The items to measure the four first order factors of CFIP were taken from Smith et al.'s [18] scale. Because online entities other than companies can ask for personal information, the word 'companies' was changed to 'organisations' in the CFIP items. Trust measures were developed based on items from Fuller et al. [73] and the risk items were taken from LaRose and Rifon [74].

Measures for privacy-protecting behaviours were developed for this study. Facebook was chosen as the specific object of trust, risk and behaviours because of its becoming a mass phenomenon [75] and the amount of personal information that is potentially shared through this social media site. Table 3 summarises the sources of the survey items.

The measures were developed, refined and ultimately validated during a pilot test phase that included five different data collections from undergraduate students over a period of 11 months at two major U.S. universities, one in the Midwest and one in the West.[4] The students were taking a required introductory Information Systems course in the business schools of the respective institutions. Data from the five student samples (summarised in Table 4) were used to validate the scales for the final measurement model. During this iterative item development process, each measurement model was assessed by looking at the reliability of the indicators, the internal reliability of the measurement scales and the discriminant validity of the indicators. In completing each assessment of the measures, any items with questionable validity were reviewed for face validity (to ensure that they were not essential to the meaning of the construct); if they were non-essential, we removed them and re-ran the PLS analysis. Some items were carefully reworded for clarity, and another group of students was then asked to respond to the revised items, and we then subjected their responses to the

**Table 3.** Sources for measurement items.

| Construct | Source |
|---|---|
| Privacy awareness | Based on Smith et al.'s [18] |
| Media privacy awareness | single item measures for |
| Personal privacy experience | Privacy Awareness and Privacy Experience |
| Concern for information privacy (second order) | [18] |
| Collection | |
| Errors | |
| Secondary use | |
| Unauthorised access | |
| Trust | Based on Fuller et al. [73] |
| Risk of information disclosure | [74] |
| Facebook behaviour | Developed for this study |

**Table 4.** Pilot phase student sample information.

| Pilot sample # | n of sample[a] | Date collected |
|---|---|---|
| 1 | 232 | March 2011 |
| 2 | 175 | September 2011 |
| 3 | 172 | November 2011 |
| 4 | 190 | January 2012 |
| 5 | 172 | February 2012 |

[a]Final sample sizes after removing responses with missing values

**Table 5.** Subject demographics.

| Demographics | Attribute | n |
|---|---|---|
| Gender | Male | 113 |
| | Female | 113 |
| Ethnicity | White | 206 |
| | Asian | 5 |
| | Hispanic | 50 |
| Age (years) | > 55 | 60 |
| | 46–55 | 90 |
| | 36–45 | 43 |
| | 18–35 | 33 |

Although this sample is skewed a bit toward older individuals, the results were qualitatively the same as those for the final student sample (see Table 4), which received the same survey instrument as the Qualtrics sample.

same PLS analysis. This process was repeated five times until we were satisfied with the properties of all the measurement items.

## 3.2. Survey implementation

The survey was implemented through the online provider Qualtrics. The sample was qualified by Qualtrics to be individuals aged over 18 years who maintained an active Facebook account. Qualtrics has a large panel of respondents recruited from various channels such as opt-in emails, co-registration, e-newsletter campaigns, internal and external affiliate networks, and social media. From this panel, the firm pre-selects potential respondents who satisfy the inclusion criteria for the specific research project (such as demographics) and sends out an email invitation to a set of potential respondents who are randomly selected from this pre-selected sample. The email invitation specifies the number of points each

**Table 6.** Factor matrix for research model.

| Factors and items | MPA | PPE | ERR | COLL | SU | UA | RSK | TR | BEH |
|---|---|---|---|---|---|---|---|---|---|
| Media privacy awareness | | | | | | | | | |
| MPA1 | 0.77 | 0.41 | 0.37 | 0.46 | 0.30 | 0.36 | 0.26 | −0.12 | 0.20 |
| MPA2 | 0.84 | 0.31 | 0.44 | 0.49 | 0.32 | 0.40 | 0.16 | −0.09 | 0.27 |
| MPA3 | 0.85 | 0.36 | 0.35 | 0.47 | 0.26 | 0.35 | 0.14 | −0.05 | 0.20 |
| MPA4 | 0.86 | 0.37 | 0.38 | 0.43 | 0.31 | 0.40 | 0.19 | −0.21 | 0.24 |
| MPA5 | 0.83 | 0.37 | 0.52 | 0.48 | 0.42 | 0.48 | 0.20 | −0.10 | 0.22 |
| Personal privacy experience | | | | | | | | | |
| PPE1 | 0.24 | 0.72 | 0.06 | 0.29 | 0.06 | 0.07 | 0.34 | −0.21 | 0.03 |
| PPE2 | 0.48 | 0.83 | 0.26 | 0.60 | 0.20 | 0.21 | 0.41 | −0.20 | 0.23 |
| PPE3 | 0.30 | 0.80 | 0.04 | 0.34 | 0.02 | 0.04 | 0.38 | −0.22 | 0.13 |
| PPE4 | 0.32 | 0.80 | 0.04 | 0.37 | 0.04 | 0.04 | 0.35 | −0.24 | 0.08 |
| Errors | | | | | | | | | |
| ERR1 | 0.37 | 0.15 | 0.69 | 0.28 | 0.34 | 0.46 | 0.08 | 0.06 | 0.18 |
| ERR2 | 0.45 | 0.13 | 0.86 | 0.34 | 0.62 | 0.66 | −0.04 | 0.07 | 0.13 |
| ERR3 | 0.43 | 0.10 | 0.82 | 0.38 | 0.53 | 0.61 | −0.02 | −0.08 | 0.13 |
| ERR4 | 0.36 | 0.09 | 0.87 | 0.37 | 0.57 | 0.62 | −0.04 | 0.10 | 0.15 |
| Collection | | | | | | | | | |
| COLL1 | 0.34 | 0.32 | 0.13 | 0.58 | 0.19 | 0.16 | 0.23 | −0.18 | 0.24 |
| COLL2 | 0.47 | 0.31 | 0.40 | 0.84 | 0.47 | 0.43 | 0.20 | −0.17 | 0.33 |
| COLL3 | 0.44 | 0.48 | 0.36 | 0.86 | 0.40 | 0.33 | 0.30 | −0.25 | 0.28 |
| COLL4 | 0.49 | 0.53 | 0.36 | 0.82 | 0.34 | 0.39 | 0.39 | −0.28 | 0.30 |
| Secondary use | | | | | | | | | |
| SU1 | 0.27 | 0.07 | 0.49 | 0.38 | 0.78 | 0.54 | −0.02 | −0.08 | 0.22 |
| SU2 | 0.32 | 0.12 | 0.56 | 0.42 | 0.85 | 0.54 | 0.01 | −0.10 | 0.23 |
| SU3 | 0.33 | 0.11 | 0.50 | 0.39 | 0.84 | 0.57 | 0.00 | −0.12 | 0.25 |
| SU4 | 0.37 | 0.08 | 0.58 | 0.37 | 0.86 | 0.75 | −0.02 | −0.14 | 0.27 |
| Unauthorised access | | | | | | | | | |
| UA1 | 0.45 | 0.11 | 0.64 | 0.41 | 0.59 | 0.85 | −0.01 | −0.07 | 0.17 |
| UA2 | 0.39 | 0.12 | 0.62 | 0.30 | 0.61 | 0.86 | 0.09 | −0.09 | 0.19 |
| UA3 | 0.41 | 0.09 | 0.65 | 0.42 | 0.70 | 0.90 | 0.04 | −0.11 | 0.22 |
| Risk | | | | | | | | | |
| RSK1 | 0.17 | 0.36 | −0.09 | 0.27 | −0.03 | 0.00 | 0.87 | −0.30 | 0.12 |
| RSK2 | 0.19 | 0.43 | 0.02 | 0.30 | 0.03 | 0.06 | 0.87 | −0.32 | 0.09 |
| RSK3 | 0.23 | 0.44 | 0.01 | 0.35 | 0.01 | 0.08 | 0.89 | −0.29 | 0.20 |
| RSK4 | 0.14 | 0.38 | −0.02 | 0.29 | 0.01 | 0.02 | 0.88 | −0.25 | 0.11 |
| RSK5 | 0.27 | 0.47 | 0.03 | 0.36 | −0.02 | 0.08 | 0.90 | −0.31 | 0.18 |
| RSK6 | 0.17 | 0.38 | −0.05 | 0.25 | −0.12 | −0.05 | 0.79 | −0.13 | 0.08 |
| Trust | | | | | | | | | |
| TR1 | −0.14 | −0.24 | 0.04 | −0.28 | −0.14 | −0.13 | −0.33 | 0.91 | −0.25 |
| TR2 | −0.12 | −0.25 | 0.04 | −0.23 | −0.12 | −0.11 | −0.29 | 0.94 | −0.21 |
| TR3 | −0.13 | −0.26 | 0.03 | −0.28 | −0.12 | −0.09 | −0.31 | 0.95 | −0.19 |
| TR4 | −0.13 | −0.27 | 0.06 | −0.25 | −0.12 | −0.07 | −0.27 | 0.94 | −0.17 |
| Behaviour | | | | | | | | | |
| BEH1 | 0.15 | 0.13 | 0.14 | 0.23 | 0.16 | 0.17 | 0.18 | −0.07 | 0.69 |
| BEH2 | 0.29 | 0.25 | 0.13 | 0.34 | 0.24 | 0.16 | 0.17 | −0.25 | 0.82 |
| BEH3 | 0.19 | 0.01 | 0.09 | 0.25 | 0.23 | 0.17 | 0.05 | −0.19 | 0.79 |
| BEH4 | 0.18 | 0.10 | 0.19 | 0.29 | 0.26 | 0.19 | 0.09 | −0.13 | 0.76 |

respondent would earn from completing the survey, where these points can be used for purchasing merchandise and services online. The survey remains open until the project quota is reached. Descriptive information concerning the 226 subjects who completed the survey, all of whom were from the USA, is shown in Table 5.

## 4. Analysis

### *4.1. Statistical analysis*

We utilised the PLS technique – specifically, SmartPLS version 2.0.M3 [76] – to analyse the data. Given our sample size and the complexity of the theoretical model, the use of PLS is appropriate [77]. The analysis both confirmed the measurement model and tested the hypotheses in the causal model.

**Table 7.** Reliability estimates and validity coefficients.

| Latent construct | AVE | CR | MPA | PPE | ERR | COLL | SU | UA | TR | RSK | BEH |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Media privacy awareness | 0.69 | 0.89 | **0.83** | | | | | | | | |
| Personal privacy experience | 0.62 | 0.87 | 0.44 | **0.79** | | | | | | | |
| Errors | 0.66 | 0.88 | 0.49 | 0.14 | **0.81** | | | | | | |
| Collection | 0.62 | 0.86 | 0.56 | 0.53 | 0.42 | **0.79** | | | | | |
| Secondary use | 0.69 | 0.90 | 0.39 | 0.11 | 0.64 | 0.47 | **0.83** | | | | |
| Unauthorised access | 0.76 | 0.90 | 0.48 | 0.12 | 0.73 | 0.44 | 0.73 | **0.87** | | | |
| Trust (general) | 0.87 | 0.97 | −0.14 | −0.27 | 0.05 | −0.28 | −0.13 | −0.11 | **0.93** | | |
| Risk (general) | 0.75 | 0.95 | 0.23 | 0.47 | −0.01 | 0.35 | −0.01 | 0.05 | −0.32 | **0.87** | |
| Behaviour | 0.59 | 0.85 | 0.27 | 0.17 | 0.18 | 0.37 | 0.29 | 0.22 | −0.22 | 0.15 | **0.77** |

We confirmed the measurement model through PLS by testing for item and scale reliability, internal consistency and convergent/discriminant validity. Table 6 shows the loadings of all indicators on their intended constructs as well as their cross-loadings on other constructs for the research model.

For adequate item reliability, ideally, the item loadings should be higher than 0.707. However, slightly lower loadings for individual items are usually acceptable provided that loadings for other items measuring the construct are greater than 0.707 [77]. In the model, 35 of the 38 item loadings exceeded 0.707. Two of the three below 0.707 were items from the established CFIP scales and were retained. The other, from the behaviour scale, was very close at 0.69. After reviewing it from a face validity basis and re-running the model to ensure there were no differences in the structural model results, we decided to retain the item in an effort to capture as much of the meaning of the behaviour construct as possible.[5]

To assess scale reliability and internal consistency, we considered the composite reliability (CR) score and the average variance extracted (AVE). For adequate reliability, the CR score should be greater than 0.70 in exploratory research or 0.80 in more mature streams of research [78]. All of our CR scores exceeded 0.85. In addition, all AVE scores exceeded the recommended level of 0.50 [77]. The AVEs for the first order factors were in the range of 0.59–0.87. The AVE for CFIP of 0.68 was calculated by averaging the R-squared values of the four reflective first order constructs. The CR and AVE scores for the first order factors are shown in Table 7.

We performed two tests for discriminant validity. First, we examined the cross-loadings of the items (see Table 6) to ensure that: (1) each item loaded more highly on its own construct than on any other construct; and (2) there were no items that loaded more highly on a construct than the items intended to measure that construct. All measures passed both of these tests. Second, we compared the square root of each construct's AVE to the correlations between that construct and all other constructs to ensure that the square roots of the AVEs exceeded the other correlations. All measures passed this test as well. The square roots of the AVEs are in bold on the diagonal in Table 7.

We used two tests for common methods bias (CMB). First, we performed Harman's one-factor test as described by Podsakoff et al. [79] and found that the measures loaded on seven separate factors with an Eigenvalue greater than 1 and that none of the factors that were extracted explained more than 26.4% of the overall variance. Second, we performed a more rigorous test for CMB proposed by Podsakoff et al. [79] and adapted for PLS by Liang et al. [80]. We tested alternative PLS models to look for CMB in the model. The original constructs became second order constructs reflected by a set of single-indicator constructs, one for each of their original indicator variables. We included a methods construct in each model measured by every indicator in that model. We also added paths in each model relating the methods construct to every first order indicator construct. We then compared each indicator's variance explained by the original constructs with that explained by the methods construct. The original constructs explain on average 70% of the variance in the indicators for the model in contrast to an average of 1% explained by the method construct. Based on the results of these two tests, we concluded that common method bias was not a significant concern.

## 5. Results

Table 8 and Figure 2 show the results of the test of our model. As the findings reveal, PA influences CFIP ($P < 0.001$), providing strong support for H1. Regarding demographics, we find strong support for the hypothesis about the effect of gender on CFIP (H2a; $P < 0.01$); female respondents have significantly higher concern for information privacy as measured by CFIP compared to male respondents. We found only a marginal relationship between age and CFIP (H2b; $P < 0.10$). The three antecedents combined to explain 33% of the variance in CFIP.

**Table 8.** Hypotheses test results.

| Hypothesis | Relationship | Path estimate | T stat | Significance level | Supported |
|---|---|---|---|---|---|
| H1 | PA -> CFIP | 0.54 | 12.91 | < 0.001 | Yes |
| H2a | Gender -> CFIP | − 0.15 | 2.81 | < 0.01 | Yes |
| H2b | Age -> CFIP | 0.10 | 1.76 | < 0.10 | Marginal |
| H3 | CFIP -> BEH | 0.29 | 3.69 | < 0.001 | Yes |
| H4 | RSK -> TR | − 0.32 | 5.17 | < 0.001 | Yes |
| H5 | TR -> BEH | − 0.18 | 2.68 | < 0.01 | Yes |

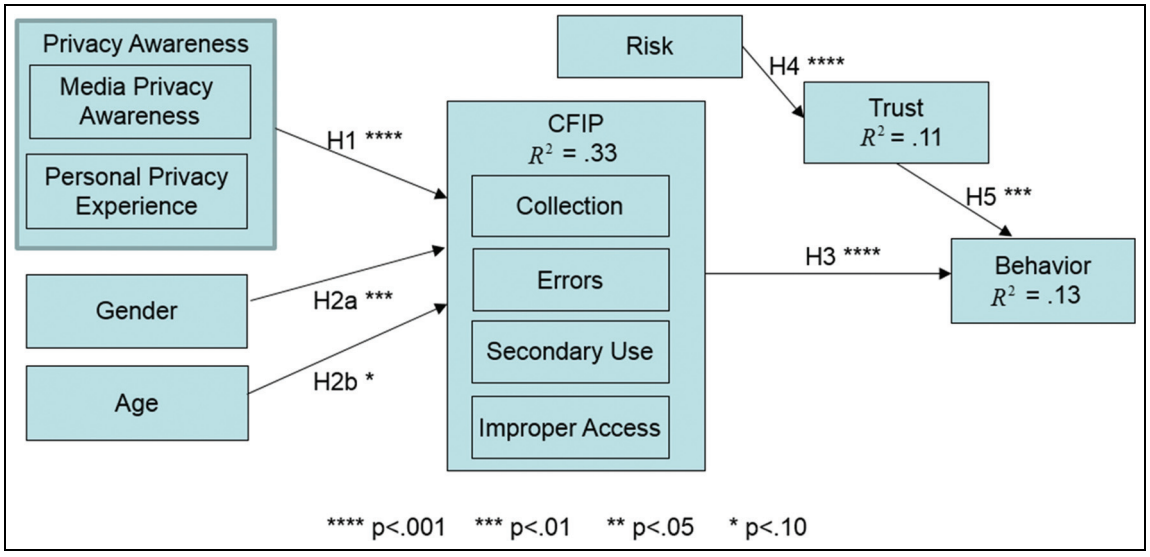


**Figure 2.** Final path model.

CFIP strongly influences privacy-protecting behaviours ($P < 0.001$), supporting H3. As expected, increased perceptions of risk have an inverse relationship with trust ($P < 0.001$) and explained 11% of the variance in trust, supporting H4. Finally, increased trust also leads to fewer privacy-protecting behaviours ($P < 0.001$), which supports H5. Trust and CFIP together account for 13% of the variance in privacy-protecting behaviour on Facebook.

## 6. Discussion

Using a sample of Facebook users provided by Qualtrics, this study has provided support for the validity of the APCO framework in explaining the relationships between some antecedents, CFIP, trust, risk and some online behaviours. The study has implications for the information privacy research stream and for managerial practice. We discusss each.

### *6.1. Implications for research*

We look across this study's four research questions so that we can place the study's contributions into perspective and reflect on future research initiatives that will deepen our understanding.

Regarding our first research question ('To what extent does the APCO framework provide an adequate nomological representation of the relationships associated with… CFIP?'), our conclusion is that, based on the subset of the constructs from within the framework that we tested, the APCO framework does indeed provide useful guidance to researchers. Overall, our tested model explained 33% of the variance in CFIP and 13% of the variance in reported privacy-protecting behaviours.

Obviously, future research initiatives would be appropriate on both sides of the CFIP construct. On the left side, it would behoove future researchers to expand the examination of antecedents to include individual factors such as

personality differences and, additionally, organisational/societal factors such as culture or climate. On the right side, a number of different outcomes should be considered: for example, different regulatory structures (and preferences associated therewith), purchasing behaviours, disclosures of personal information (online and offline), consumer defections, etc. (see Smith et al. [7], from which many of these examples are taken, for additional discussion.) Consideration of the APCO framework at other levels of analysis (group, organisational, societal) would also be appropriate.

Regarding our second research question ('What is the relationship between PA and CFIP?'), the answer is 'a strong one' ($P < 0.001$ for H1). Future research could profitably consider a more specific model that tests PA, CFIP and outcomes all within the specific domain of a certain type of interchange (e.g. medical, financial, consumer). In that context, in fact, one might find that CFIP is best viewed as a dual construct with both general and specific components (see Li [5] for a model that considers this duality).

Regarding our third research question ('What are the roles of trust and risk in the APCO framework?'), perceived risk is seen to affect trust ($P < 0.001$ for H4), which in turn is seen to affect privacy-protecting behaviours ($P < 0.001$ for H5). These are important results, as they shed additional light on what is clearly a complex relationship between risk and trust, not only in the domain of privacy research but in the broader research stream [70]. Even so, our findings should be taken neither as confirmation nor refutation of other studies but, rather, as exploratory results that warrant attempts at replication.

Regarding our fourth research question ('What is the relationship between CFIP and privacy-protecting behaviours?'), the relationship appears to be a strong and significant one ($P < 0.001$ for H3). This strong result serves as an especially potent warning for executives who labour in industries that may be forced to deal with consumer reactions to perceived privacy violations. This leads to some important implications for practice, to which we now turn.

## 6.2. Implications for practice

While many of the findings of this study will be of greater import to researchers than practitioners, there nevertheless are three areas that have implications for managers.

First, as noted above, the tight linkage between CFIP and privacy-protecting behaviours should serve as a wake-up call to executives in information-intensive industries. As just one example, Facebook's user base is in decline [81] and researchers recently documented that one half of those who quit Facebook have done so because of their concerns about privacy [82]. This phenomenon is not strictly one associated with social media, however, and recent revelations regarding governmental surveillance, which reportedly has extended into the commercial arena [83], can only be expected to increase privacy concerns. Based on the findings in this study, these increased concerns can only lead to problems for commercial and non-commercial entities that rely on individuals to willingly share personal information and embrace activities that use such information. Most challenging to executives, however, is that it is increasingly becoming the case that actions taken by an individual entity can have only a muted impact on the overall level of privacy concerns. Executives and their industry compatriots would be well advised to consider consolidated efforts to create policies and regulatory mechanisms that will ameliorate concerns. Further, they may band together to lobby governmental entities for restrictions on data collection and sharing; some efforts in this direction are already occurring [84] and more such initiatives are advised.

Second, it is instructive to note that perceived risk affects trust, which in turn affects individuals' privacy-protecting behaviours. It is obvious that organisations dealing in individually identifiable personal information should engage in trust-building and risk-mitigating activities. Trust-building activities usually involve the creation of privacy-protection policies and mechanisms, which are communicated clearly to individuals who engage in transactions with an organisation. In an online context, these policies/mechanisms are usually communicated on a website and individuals are often allowed to indicate their preferences as they engage with the organisation. Organisations often grapple with the distinction between offering individuals the ability to 'opt in' or to 'opt out' of secondary data uses (in practical terms, this often equates to whether a 'You may use this data for secondary purposes' box is presented in default mode as checked or unchecked). Although we are unaware of studies supporting this contention, we postulate that trust will be more easily gained by allowing individuals to 'opt in' rather than forcing them to 'opt out'.

With respect to risk mitigation, the oft-cited 'Fair Information Practices' [12] include 'inspection' and 'correction' as salient activities. Individuals who provide data to organisations should perceive their risk as being dampened when they are allowed to inspect any data associated with their record and to request correction of data elements they believe are in error. In our experience, most American firms have a procedure for inspection but not correction, whereas most European firms (largely due to the different regulatory structure) also offer a correction option. In our view, organisations around the world would be well served by a more 'European' approach in which both inspection and correction are provided, even if this is not legally mandated.

Third, PA is an important factor in determining individuals' level of privacy concern, which manifests itself in behavioural actions. It appears that the more individuals experience what they perceive as privacy violations, and the more

they hear about such violations, the more they engage in privacy-protecting behaviours. In many situations, those behaviours may actually have benefits for organisations that deal with the individuals, but to the extent that the individuals withdraw from certain interactions with organisations due to their concerns, this may become dysfunctional. This suggests that, in addition to direct benefits from trust-building and risk-mitigation strategies (see above), firms should endeavour to avoid negative privacy experiences for their customers. Executives should lobby for the creation of auditable privacy policies across their industries. In some industries (e.g. direct marketing), industry organisations have long provided leadership and guidance in this domain. In other industries, such efforts are non-existent or in their infancy. Enlightened managers will prod their industry colleagues to take the necessary steps regarding privacy-related matters. Additionally, there may be real benefits to organisations' making the populace aware of those policies/practices, thus leading to fewer media reports of privacy violations and more of positive privacy-protecting activities.

### *6.3. Limitations*

There are four potential limitations to this study. First, our model is not exhaustive because of the large number of antecedents and outcomes that might be included across the entire APCO framework. As was noted above (under 'Implications for Research'), much additional work should be done to include additional constructs.

Second, although going beyond what has been traditionally examined in most privacy research papers (behavioural intentions), this study relies on self-reported rather than measured behaviours. It is conceivable that individuals may misreport their own behaviours, either due to cognitive constraints or in an attempt at self-justification. It should be noted, however, that our Facebook-related survey items are quite specific and are less likely to be subject to such misreporting than are general self-reported items.

Third, although our newly developed measures for several constructs proved to have both convergent and discriminant validity, our items for some constructs such as PA and Facebook-specific behaviours were created for this study with – in the case of PA – some inspiration from prior studies. These items should be viewed not as comprising fully validated scales but, rather, as exploratory contributions to a growing research stream. Future researchers will no doubt wish to refine our items and purify the scales. Also, the data used in the analysis for this study are from one point in time. Future research may examine whether and how the relationships among the constructs have evolved over time.

Finally, our use of a U.S.-based sample could be considered a limitation. However, to our knowledge there are no international organisations that provide cross-cultural, random samples from multiple continents, so construction of a worldwide sample would require merging datasets collected through disparate means. Thus, to secure an international sample using a similar sampling technique (which allowed us to secure a non-student sample with varied demographics) would be very difficult. We believe that the benefit of being able to generalise from a broad-based, non-student sample (albeit from within a single culture) justifies our approach.

## 7. Conclusion

Since the early 1970s, worldwide concerns about information privacy have continued to rise and researchers (especially since the 1990s) have paid growing attention to the topic of information privacy. Recently, some attempts to provide overarching reviews of the research [5–7] have yielded some intriguing suggestions for a research agenda.

In this paper, we have attempted to ascertain the validity of one suggested framework – APCO, as proposed by Smith et al. [7] – and to consider some of the implications associated therewith. This study should be viewed most directly as an 'informing event' for future work. We hope that other researchers will join us as we attempt to unravel some of the important (and, in many cases, under-studied) relationships inherent in this complex research domain.

### Funding

Zafer D. Ozdemir gratefully acknowledges research support by Farmer School of Business, Miami University.

### Notes

1. To the best of our knowledge, comparable public opinion surveys have not been conducted in recent years.
2. We use the phrase 'almost uniformly' because some minor perturbations are sometimes noted: in [65, Tables 1 and 2], the percentage for ages 18–24 years was 47%, whereas the percentage for ages 25–29 years was 45%, with consistent increases from that bracket upwards; in [66], the value for ages 18–29 years was 37%, which increased to 51% for ages 30–49 years but dropped slightly to 49% for ages 50–64 years. Otherwise, the consistent pattern of increasing percentages for 'very concerned' for

increasing ages was consistent in [65–68]. Note that the upward trend seems to dissipate for the age bracket 65 + years, which consistently yields a lower 'very concerned' percentage than ages 50–64 years.

3. Bélanger and Crossler [6, p. 1020] noted that the Internet user's information privacy concerns (IUIPC) scale, developed by Malholtra et al. [33], 'explains more of the variance *in a person's willingness to transact* [italics added] than CFIP', according to its developers, and Bélanger and Crossler [6, p. 1020] argued for IUIPC's widespread use. As they also noted, however, CFIP's use 'could be' because 'CFIP is viewed as the *de facto* [italics in original] measure for information privacy concerns'. The context of the claim regarding IUIPC's explanatory power ('in a person's willingness to transact') limits its domain more narrowly than the domain of this study. Even so, in the early iterations of our testing with student subjects (see below), we included both CFIP and IUIPC in our survey, and we found that CFIP's measurement properties and predictive power far exceeded IUIPC's in this context.
4. We gratefully acknowledge Gove Allen and Nick Ball of Brigham Young University for their assistance in data collection.
5. We re-ran the model without the items and observed no meaningful differences in the structural model results.

## References


[1] Joinson AN, Paine C, Buchanan T and Reips U-D. Watching me, watching you: privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom. *Journal of Information Science* 2006; 32: 334–343.

[2] Consumers Union. *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*. Yonkers, NY: Consumers Union, 2008.

[3] Gomez J, Pinnick T and Soltani A. *KnowPrivacy: The Current State of Web Privacy, Data Collection, and Information Sharing*. Berkeley, CA: UC Berkeley School of Information, 2009.

[4] Bailey SGM and Caidi N. How much is too little? Privacy and smart cards in Hong Kong and Ontario. *Journal of Information Science* 2005; 31: 354–364.

[5] Li Y. Empirical studies on online information privacy concerns: literature review and an integrative framework. *Communications of the Association for Information Systems* 2011; 28: 453–496.

[6] Bélanger F and Crossler R. Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly* 2011; 35: 1017–1041.

[7] Smith HJ, Dinev T and Xu H. Information privacy research: an interdisciplinary review. *MIS Quarterly* 2011; 35: 989–1015.

[8] Pavlou P. State of the information privacy literature: where we are now and where should we go? *MIS Quarterly* 2011; 35: 977–988.

[9] Bellman S, Johnson EJ, Kobrin SJ and Lohse GL. International differences in information privacy concerns: A global survey of consumers. *Information Society* 2004; 20: 313–324.

[10] Campbell AJ. Relationship marketing in consumer markets. *Journal of Direct Marketing* 1997; 11: 44–57.

[11] Cho H, Rivera-Sanchez M and Lim SS. A multinational study on online privacy: global concerns and local responses. *Media & Society* 2009; 11: 395–416.

[12] Culnan MJ. How did they get my name? an exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly* 1993; 17: 341–363.

[13] Dinev T, Bellotto M, Hart P, Russo V, Serra I and Colautti C. Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*. 2006; 15: 389–402.

[14] Dinev T and Hart P. Internet privacy concerns and their antecedents – measurement validity and a regression model. *Behavior and Information Technology* 2004; 23: 413–423.

[15] Hwang HG, Han HE, Kuo KM and Liu CF. The differing privacy concerns regarding exchanging electronic medical records of Internet users in Taiwan. *Journal of Medical Systems* 2012; 36: 3783–3793.

[16] Lu Y, Tan BCY and Hui K-L. Inducing customers to disclose personal information to internet businesses with social adjustment benefits. In: *ICIS 2004: Twenty-Fifth International Conference on Information Systems*. Washington, DC, 2004, pp. 272–281.

[17] Nowak GJ and Phelps J. Understanding privacy concerns: an assessment of consumers's information-related knowledge and beliefs. *Journal of Direct Marketing* 1992; 6: 28–39.

[18] Smith HJ, Milberg JS and Burke JS. Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*. 1996; 20: 167–196.

[19] Xu H. The effects of self-construal and perceived control on privacy concerns. In: *Proceedings of 28th Annual International Conference on Information Systems (ICIS 2007)*. Montréal, 2007.

[20] Xu H, Dinev T, Smith HJ and Hart P. Examining the formation of individual's information privacy concerns: toward an integrative view. In: *29th International Conference on Information Systems*. Paris, 2008.

[21] Xu H, Teo HH, Tan BCY and Agarwal R. Research note – effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research* 2013; 23: 1342–1363.

[22] Yao M. Predicting user concerns about online privacy in Hong Kong. *Cyberpsychology & Behavior* 2008; 11: 779–781.

[23] Yao MZ, Rice RE and Wallis K. Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology* 2007; 58: 710–722.

[24] Anderson CL and Agarwal R. The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research* 2011; 22: 469–490.
[25] Cha J. Exploring the internet as a unique shopping channel to sell both real and virtual items: a comparison of factors affecting purchae intention and consumer characteristics. *Journal of Electronic Commerce Research* 2011; 12: 115–132.
[26] Culnan MJ and Armstrong PK. Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation. *Organization Science* 1999; 10: 104–115.
[27] Dinev T, Bellotto M, Hart P, Russo V, Serra I and Colautti C. Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management* 2006; 14: 57–93.
[28] Dinev T, Hart P and Mullen MR. Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *Journal of Strategic Information Systems* 2008; 17: 214–233.
[29] Eastlick MA, Lotz SL and Warrington P. Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research* 2006; 59: 877–886.
[30] Frye NE and Dornisch MM. When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Computers in Human Behavior* 2010; 26: 1120–1127.
[31] Hong W and Thong JYL. Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quarterly* 2013; 37: 275–298.
[32] Lowry PB, Cao J and Everard A. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the case of instant messaging in two cultures. *Journal of Management Information Systems* 2011; 27: 163–200.
[33] Malhotra KN, Kim SS and Agarwal J. Internet users' information privacy concerns (iuipc): the construct, the scale, and a causal model. *Information Systems Research* 2004; 15: 336–355.
[34] Metzger MJ. Privacy, trust, and disclosure: exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication* 2004; 9: 00.
[35] Milne GR and Boza M-E. Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing* 1999; 13: 5–24.
[36] Mothersbaugh DL, Foxx WK, Beatty SE and Wang S. Disclosure antecedents in an online service context: the role of sensitivity of information. *Journal of Service Research* 2012; 15: 76–98.
[37] Sheehan KB and Grubbs-Hoy M. Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising* 1999; 28: 37–51.
[38] Son JY and Kim SS. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly* 2008; 32: 503–529.
[39] Taddei S and Contena B. Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior* 2013; 29: 821–826.
[40] Tan X, Qin L, Kim Y and Hsu J. Impact of privacy concern in social networking web sites. *Internet Research* 2012; 22: 211–233.
[41] Van Slyke C, Shim JT, Johnson R and Jiang J. Concern for information privacy and online consumer purchasing. *Journal of the Association of Information Systems* 2006; 7: 415–444.
[42] Walgrave M and Heirman W. Adolescents, online marketing and privacy: predicting adolescents' willingness to disclose personal information for marketing purposes. *Children & Society* 2013; 27: 434–447.
[43] Xu Y, Tan B, Hui K and Tang W. Consumer trust and online information privacy. In: *Proceedings of the Twenty-Fourth Annual International Conference on Information Systems (ICIS)*. Seattle, WA, 2003, pp. 538–548.
[44] Zhou T. An empirical examination of user adoption of location-based services. *Electronic Commerce Research* 2013; 13: 25–39.
[45] Bansal G, Zahedi F and Gefen D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems* 2010; 49: 138–150.
[46] Chechen L, Chuang-Chun L and Kuanchin C. Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications* 2011; 10: 702–715.
[47] Dinev T and Hart P. Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce* 2005; 10: 7–29.
[48] Mohamed N and Ahmad IH. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior* 2012; 28: 2366–2375.
[49] Okazaki S, Li H and Hirose M. Consumer privacy concerns and preference for degree of regulatory control. *Journal of Advertising* 2009; 38: 63–77.
[50] Stewart KA and Segars AH. An empirical examination of the concern for information privacy instrument. *Information Systems Research* 2002; 13: 36–49.
[51] Compeau D, Marcolin B, Kelley H and Higgins C. Research commentary – generalizability of information systems research using student subjects – a reflection on our practices and recommendations for future research. *Information Systems Research* 2012; 23: 1093–1109.

[52] Xu H, Dinev T, Smith HJ and Hart P. Information privacy concerns: linking individual perceptions with institutional privacy assurances. *Journal of the Association of Information Systems* 2011; 12: 798–824.
[53] Bansal G, Zahedi F and Gefen D. The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: a multiple-context investigation. In: *29th Annual International Conference on Information Systems (ICIS 2008)*. Paris, 2008.
[54] Schoenbachler DD and Gordon GL. Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing* 2002; 16: 2–16.
[55] Xu H, Teo HH and Tan BCY. Predicting the adoption of location-based services: the roles of trust and privacy risk. In: *Proceedings of 26th Annual International Conference on Information Systems (ICIS 2005)*. Las Vegas, NV, 2005, pp. 897–910.
[56] Sheehan KB. Toward a typology of internet users and online privacy concerns. *The Information Society* 2002; 18: 21–32.
[57] Pavlou P and Fygenson M. Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior. *MIS Quarterly* 2006; 30: 115–143.
[58] Westin AF. *Consumer Privacy Issues in the Nineties*. Atlanta, GA: Equifax Inc., 1990.
[59] Stone EF and Stone DL. Privacy in organizations: theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management* 1990; 8: 349–411.
[60] Phelps J, Nowak G and Ferrell E. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy and Marketing* 2000; 19: 27–41.
[61] Culnan MJ. Consumer awareness of name removal procedures: implication for direct marketing. *Journal of Interactive Marketing* 1995; 9: 10–19.
[62] Hoofnagle C, King J, Li S and Turow J. How different are young adults from older Americans when it comes to information privacy attitudes and policies? 2010. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864
[63] Metzger MJ. Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication* 2007; 12: 335–361.
[64] Sheehan KB. An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing* 1999; 13: 24–38.
[65] Equifax Inc. *Equifax-Harris Consumer Privacy Survey 1994*. New York, NY: Louis Harris and Associates, 1994.
[66] Equifax Inc. *Equifax-Harris Mid-Decade Consumer Privacy Survey 1995*. New York, NY: Louis Harris and Associates, 1995.
[67] Equifax Inc. *Harris-Equifax Health Information Privacy Survey 1993*. New York, NY: Louis Harris and Associates, 1993.
[68] Equifax Inc. *The Equifax Report on Consumers in the Information Age*. Atlanta, GA: Equifax Inc., 1990.
[69] Regan PR, FitzGerald G and Balint P. Generational views of information privacy? *Innovation: The European Journal of Social Science Research* 2013; 26: 81–99.
[70] Mayer RC, Davis JH and Schoorman FD. An integrative model of organizational trust. *Academy of Management Review* 1995; 20: 709–734.
[71] Yates JF and Stone ER. The risk construct. In: Yates JF (ed.) *Risk-Taking Behavior*. Chichester: Wiley, 1992, pp. 1–25.
[72] Dinev T and Hart P. An extended privacy calculus model for E-commerce transactions. *Information Systems Research* 2006; 17: 61–80.
[73] Fuller MA, Serva MA and Benamati JH. Seeing is believing: the transitory influence of reputation information on e-commerce trust and decision-making. *Decision Sciences* 2007; 38: 675–699.
[74] Larose R and Rifon NJ. Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs* 2007; 41: 127–149.
[75] Carmagnola F, Osborne F and Torre I. Escaping the Big Brother: An empirical study on factors influencing identification and information leakage on the Web. *Journal of Information Science* 2014; 40: 180–197.
[76] Ringle CM, Wende S and Will A. *SmartPLS 2.0.M3* 2005. Hamburg: SmartPLS. Available at: http://www.smartpls.com
[77] Chin WW and Newsted PR. Structural equation modeling analysis with small samples using partial least squares. In: Hoyle R (ed.) *Statistical Strategies for Small Sample Research*. Thousand Oaks, CA: Sage Publications, 1999, pp. 307–341.
[78] Fornell C and Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 1981; 18: 39–50.
[79] Podsakoff P, MacKenzie S, Lee J and Podsakoff N. Common method bias in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology* 2003; 88: 879–903.
[80] Liang H, Saraf N, Hu Q and Xue Y. Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS Quarterly* 2007; 31: 59–87.
[81] Garside J. Facebook loses millions of userss as biggest markets peak. *The Guardian*. London: The Guardian, 2013.
[82] Munson L. Half of Facebook-quitters leave over privacy concerns. *NakedSecurity*, 2013.
[83] CBS News. NSA surveillance exposed. New York: CBS News, 2013.
[84] Kang C and Nakashima E. Tech executives to Obama: NSA spying revelations are hurting business. *Washington Post*. Washington, DC: Washington Post, 2013.

## Appendix A: Items from Instrument

### *Media Privacy Awareness (Scale Strongly Disagree → Strongly Agree)*

PA1: Almost every day, I hear or read something about the invasion of people's information privacy.
PA2: There is almost always something in the news about the use or misuse of consumers' information.
PA3: I frequently hear or read about the invasion of information privacy.
PA4: Lots of news articles are being written about how consumers' information is being used or misused.
PA5: The topic of information privacy has been in the news a lot.

### *Personal Privacy Experience (Scale Strongly Disagree → Strongly Agree)*

PE1: I have frequently been the victim of improper invasions of my information privacy.
PE2: I often feel that my information privacy is being violated.
PE3: My information privacy is invaded all the time.
PE4: My information privacy has not been protected well.

### *CFIP – Collection (Scale Strongly Disagree → Strongly Agree)*

COL1: It usually bothers me when organisations ask me for personal information.
COL2: When organisations ask me for personal information, I sometimes think twice before providing it.
COL3: It bothers me to give personal information to so many organisations.
COL4: I am concerned that organisations are collecting too much personal information about me.

### *CFIP – Errors (Scale Strongly Disagree → Strongly Agree)*

ERR1: All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.
ERR2: Organisations should take more steps to make sure that the personal information in their files is accurate.
ERR3: Organisations should have better procedures to correct errors in personal information.
ERR4: Organisations should devote more time and effort to verifying the accuracy of the personal information in their databases.

### *CFIP – Secondary Use (Scale Strongly Disagree → Strongly Agree)*

SU1: Organisations should not use personal information for any purpose unless it has been authorised by the individuals who provided the information.
SU2: When people give personal information to an organisation for some reason, the organisation should never use the information for any other reason.
SU3: Organisations should never sell the personal information in their computer databases to other companies.
SU4: Organisations should never share personal information with other companies unless it has been authorised by the individuals who provided the information.

### *CFIP – Improper Access (Scale Strongly Disagree → Strongly Agree)*

UA1: Organisations should devote more time and effort to preventing unauthorised access to personal information.
UA2: Computer databases that contain personal information should be protected from unauthorised access – no matter how much it costs.
UA3: Organisations should take more steps to make sure that unauthorised people cannot access personal information in their computers.

### *Trust (Scale Strongly Disagree → Strongly Agree)*

Each statement was used twice, once followed by Facebook and once followed by online companies (in general)

T1: When it comes to sharing my personal information online and knowing it will be protected, I feel comfortable with Facebook
T2: When it comes to sharing my personal information online and knowing it will be protected, I can rely on Facebook
T3: When it comes to sharing my personal information online and knowing it will be protected, I can count on Facebook
T4: When it comes to sharing my personal information online and knowing it will be protected, I can depend on Facebook

### *Risk of Information Disclosure (Scale not at all → To a great extent)*

To what extent do you believe that you face each of the risks below when you use Facebook?
R1: I will be the victim of an online scam.
R2: Information will be captured that could be used against me in my future life.
R3: Someone will hack into the site and steal my personal information.
R4: Someone will use the information to harass me.
R5: My identity will get stolen.
R6: I will get unauthorised charges on my credit card.

### *Facebook Behaviour (Scale not at all → To a great extent)*

FB1: To what extent do you currently limit access to your personal information/content (beyond the default settings) in Facebook?
FB2: To what extent do you avoid 'friending' some people on Facebook?
FB3: To what extent do you limit what you post on Facebook?
FB4: To what extent do you avoid using third party applications on Facebook?