An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps

Usman Aleem, Hasan Cavusoglu, Izak Benbasat

Sauder School of Business, University of British Columbia

May 2017

Abstract

In this paper, we contend that transacting for digital goods – anything that can be stored, delivered and used in its electronic format online – introduces privacy uncertainty in the minds of consumers. Privacy uncertainty – a consumer's inability to assess the privacy of the data she entrusts to the seller of a digital good – acts as a friction in marketplaces in which digital goods are sold. We extend the existing literature on seller and product uncertainties by incorporating privacy uncertainty, and theorize and empirically test the antecedents and consequences of privacy uncertainty. We distinguish two classes of information asymmetry as antecedents of privacy uncertainty: pre-purchase and post-purchase asymmetries. While hidden information and hidden action were identified as pre-purchase and post-purchase asymmetries respectively, we argue that hidden effort which is unique to information privacy as another dimension of post-purchase information asymmetry as it only arises when consumers' data is stored and used over an extended period of time.

Using a factorial survey method, we tested our theoretical model in the context of buying a mobile app. We show that a subject's privacy uncertainty significantly influences her willingness to buy an app above and beyond the subject's seller and product uncertainties. In addition, our results show that post-purchase information asymmetry, especially the perception of hidden action, leads to higher privacy uncertainty, a result that challenges the efficacy of the contemporary practice of using "notice and consent" in the online markets.

Keywords: *Privacy, privacy uncertainty, information asymmetry, digital goods, mobile apps.*

1 Introduction

Since the Internet has emerged as an alternative sales channel for physical goods, scholars have studied potential sources of friction in the online marketplace. Motivated by the lack of face-to-face interactions with the sellers and the sheer number of vendors offering products online, a rich body of literature has focused on understanding and reducing *seller uncertainty* and helping buyers assess the reliability of vendors (Featherman and Pavlou 2003; Gefen et al. 2003; Jarvenpaa and Staples 2000; Pavlou and Fygenson 2006; Pavlou et al. 2007). A related stream of research has investigated the impact of *product uncertainty*, or the buyer's inability to verify the quality of the physical goods in online markets (Dimoka and Pavlou 2008; Dimoka et al. 2012; Ghose 2009).

Due to advances in Internet and mobile technologies and the introduction of new business models, *digital goods*, or anything that can be stored, delivered and used in its electronic format online, are now indispensible parts of our lives. News portals, video-sharing platforms, social networking sites, cloud-based software, online games, and mobile applications are some popular examples. Digital goods are almost always used in a networked environment, leading to a constant transfer of generated information among consumers and the service providers. While e-commerce platforms selling physical goods require consumers to part with some personal and financial information (James 2005; Newman and Clarke 2013), the information is limited to the details specifically requested by the vendors at the time of the transaction. However, sellers can obtain more sensitive information more frequently from digital goods, to an extent that is often unknown to the consumers. While consumers purchasing digital goods (either in return for money or something else) may perceive seller and product uncertainty, we posit that they also perceive another kind of uncertainty associated with the privacy of their personal information. *Privacy uncertainty* is, therefore, defined as *a consumer's inability to assess the privacy of the information she entrusts to the seller of a digital good.* In this paper, by focusing on mobile apps marketplaces, we aim to determine the antecedents and consequences of privacy uncertainty.

Unlike a one-time information exchange involved in purchasing physical products, the information exchange in the context of digital goods is not confined to the initial sale transaction, but takes place continuously between consumers and sellers. Consumers are creating more personal content using mobile apps on their cell phones and tablets (Buck et al. 2014)[1]. In 2014, Apple's App Store sold more than 100 billion apps and Google's Marketplace sold 120 billion. Moreover, consumers' content, usage patterns and real-time locations are available to the app developers. While consumers may not voluntarily disclose such information, the proper functioning of the apps may require it. More alarmingly, the personal information that apps capture can be sold to data aggregators that compile information from various sources (Gantz and Reinsel 2012). This ability to create more accurate profiles of online customers by gathering a wide array of data has paved the way for the business of trading personal information (Buck et al. 2014). While most consumers are not fully aware of the extent of privacy threats that their personal information is facing, they are concerned about the privacy of their information. As mobile apps continue to generate rich, individually identifiable data, *will customers consider privacy uncertainty along with seller and product uncertainty when deciding whether to purchase digital goods in online markets?* This paper will shed light on this question by build upon the information systems (IS) literature on product and seller uncertainty (Dimoka et al. 2012; Ghose 2009; Pavlou et al. 2007).

The emergence of privacy uncertainty due to the changing nature of business is not the *only* reason for studying this phenomenon. The resulting rise in online information exchange has also increased opportunities for phishing (James 2005; Wall 2007), electronic theft, fraud, and espionage (Holt 2007; Holt and Graves 2007; Newman and Clarke 2013; Taylor et al. 2014; Wall 2003; Wall 2007). Given the media outcry over the privacy and security of personal information, the proliferation of "stolen data" markets (Franklin et al. 2007; Thomas and Martin 2006), and the surprising dearth of privacy-enhanced mobile apps, it is paradoxical that consumers and business organizations do not demand more transparent privacy practices from sellers of digital goods.

[1] According to Meeker and Wu (2013), global mobile traffic accounted for 15% of total internet use in 2013, and even more people will use mobile devices (vs. desktop computers) to go online by 2015.

Scholars who argue that markets respond to the needs and expectations of consumers might suggest that the lack of privacy-enhanced apps implies that customers do not care sufficiently about their privacy. However, the literature indicates that consumers value their personal information (Spiekermann et al. 2001). In fact, in return for their personal information, they request between $30.49 and $44.62, an amount far greater than the market value of their information (Hann et al. 2007). Furthermore, they have a strong preference for online retailers that do better in protecting their data (Tsai et al. 2011), and want to be compensated when their information is compromised (Hui et al. 2007). While research shows a clear potential for offering value to privacy-inclined users, we find contradictory evidence in online mobile app markets, where consumers typically buy cheap and insecure apps. Since market uncertainties have been known to negatively affect the prices paid and the frequency of transactions (Akerlof 1970), we contend that the fact that mobile app markets are not accommodating privacy-inclined customers can be explained by the underlying privacy uncertainty in these markets. Such privacy uncertainty hinders a consumer's ability to distinguish a more privacy-respectful app from the others, and consequently reduces the incentive for sellers to provide privacy-enhanced software. Hence, we ask: *What make buyers perceive privacy uncertainty?* This will be addressed in this paper by build upon the notion of information asymmetry (Akerlof 1970; Hölmstrom 1979).

Our findings indicate that post-purchase information asymmetry plays a more dominant role in reducing consumers' privacy uncertainty than pre-purchase information asymmetry. This leads to an important conclusion that the practice of "notice and consent" promoted by the FTC, which deals with pre-purchase information asymmetry only, is not effective in reducing privacy uncertainty, and hence new policies are needed to inform customers about post-purchase actions by online companies that reduce the customers' exposure to privacy loss after consent has been provided.

In the remainder of the paper, we first discuss how privacy uncertainty manifests itself in online transactions for digital goods, such as mobile apps, whose usage is likely to result in a continuous exchange of consumer information. Drawing upon agency theory, we then focus on the antecedents of

privacy uncertainty and discuss how the dimensions of *hidden information*, *hidden action*, and *hidden effort* contribute to information asymmetry. We subsequently test our theoretical model using a factorial survey.

2 Literature Review

While economics and marketing provide deep insights on the effects of information asymmetry and its consequences at the market level, in this section, we focus on information systems literature to characterize new types of information asymmetries that relate to digital goods. We describe their impact on seller, product, and privacy uncertainty and underscore the importance of privacy uncertainty in customers' online purchasing decisions.

Knight (1921) first introduced the concept of uncertainty and described it as a consequence of imperfect information. In an economic transaction, uncertainty arises due to a difference in the knowledge held by the two parties (Rindfleisch and Heide 1997). A difference in information, also called information asymmetry, exists when sellers know more about the product than consumers (Mishra et al. 1998). Many products and services have attributes whose quality can be evaluated only after they have been consumed (Nelson 1970). Hence, information asymmetry is more pronounced for experience goods (Kirmani and Rao 2000). If the information asymmetry cannot be resolved, consumers become uncertain about the actual quality of the product (Arrow 1963). Under these conditions, opportunistic sellers may make false claims about their wares, a phenomenon called *adverse selection* (Akerlof 1970). Moreover, when a seller has more information than the buyer about its actions and intentions, it has a tendency or incentive to behave inappropriately (such as reducing the product's quality) after the transaction if it can do so, leading to another phenomenon called *moral hazard* (Hölmstrom 1979; Rao et al. 1997; Rao et al. 1999).

The effects of information asymmetry are even more pronounced in e-commerce (Pavlou and Gefen 2004; Pavlou et al. 2007). Since the goods are sold online, consumers must determine their quality over the Internet; in addition, they must also determine whether the seller will complete the transaction by

shipping the product on time (Pavlou et al. 2007). This information asymmetry creates uncertainty in consumers' evaluation of the product's quality. Pavlou et al. (2007) conceptualize *seller uncertainty* in the context of e-commerce as a consumer's inability to determine whether the vendor is actually selling the product claimed. They consider the dimensions of whether the seller is presenting accurate information about the product and whether it will fulfill its claims after the sale. Moreover, consumers are also confronted with uncertainty due to the lack of transparency in the sales process (Chatterjee and Datta 2008), since they do not know how the seller will transfer the product to them. These uncertainties primarily occurred in the early days of e-commerce, trust (Pavlou and Fygenson 2006) and reputation-building mechanisms (Dellarocas 2003) have now partially mitigated customers' concerns and improved the efficiency of electronic markets. Large e-retailers like Amazon give their customers confidence that reliable sellers do exist and will honor the transaction. In addition, encryption technologies and third-party escrow (Pavlou and Gefen 2004) afford structural assurance and reduce the drawbacks of sharing financial information.

The introduction of intermediary e-commerce platforms (e.g., eBay, Amazon) allows sellers to increase the variety of products they offer, including used goods. The proliferation of goods that consumers cannot readily evaluate introduces product uncertainty (Dimoka et al. 2012; Ghose 2009). The market overcomes this inefficiency when intermediaries ensure that buyers can return the products for a full refund. In addition, the IS literature identifies many design aspects that could help sellers reduce information asymmetry regarding products (e.g., Jiang and Benbasat 2004).

More recently, researchers have examined another dimension, *product fit uncertainty*, which arises when consumers are unable to determine whether a product will meet their personal needs (Hong and Pavlou 2010; Hong and Pavlou 2014). Whereas product uncertainty relates only to the product's attributes and how it will perform, product fit uncertainty focuses on whether the product will suit a consumer's preferences. This type of uncertainty is pervasive in experience products, which can only be evaluated after they have been procured and used.

Table 1: IS Literature on Measuring Uncertainty			
Transacted Good	**Exchange**	**Transaction Type/Frequency**	**Uncertainty Measured and Context**
Physical Product	*Seller:* Product *Buyer:* Money	*Type:* Terminal *Frequency:* Repeat Business	*Seller Uncertainty:* Pavlou et al. (2007) surveyed people who bought books and prescription drugs.
Used/New Physical Product	*Seller:* Product *Buyer:* Money	*Type:* Terminal *Frequency:* Repeat Business	*Product Uncertainty:* Dimoka et al. (2012) studied used cars bought over eBay; uncertainty measured by coders. *Product Uncertainty:* Ghose (2009) studied used goods and showed that high-quality items took longer to sell. *Fit Uncertainty:* Hong and Pavlou (2010) and Hong and Pavlou (2014) examined how consumers experience uncertainty between their preferences and product attributes.
Digital Goods (such as mobile apps)	*Seller:* App *Buyer:* Money and/or Personal Information	*Type:* Terminal or Continuous *Frequency:* Repeat Business	Current research (mobile app buyers).
Note: While many papers discuss information asymmetry, this table focuses on those that explicitly operationalize a dimension of uncertainty in IS.			

The rise of digital goods calls for a deeper understanding of aspects of privacy in e-commerce markets. Privacy can be an issue for a customer purchasing a physical good from an online seller, as she must disclose some personal information during the transaction. The more information disclosure requested, the more concerned and uncertain the buyer will be about the seller. However, along with this information, the seller of a digital good can obtain additional data while the app is in use, such as the customer's content, location, and usage patterns (Gantz and Reinsel 2012). The nature, amount, and specificity of the information that the seller of the digital good can acquire during the life cycle of the product are not comparable to those of the information that it can acquire during the sales transaction (Buck et al. 2014; Gantz and Reinsel 2012). For Pavlou et al. (2007), who focused on physical goods, privacy concerns stem from the information the buyer discloses during a transaction and should hence be treated as a dimension of seller uncertainty. As physical goods do not offer continuous data-gathering possibilities, they did not explore the underlying information asymmetry concerning privacy. Let's compare a physical book and a digital book. An e-book can gather extensive consumer data about its use,

which is unavailable to the sellers of the physical equivalent. For instance, while Amazon has been selling books for over a decade, the recent inclusion of e-books offers granular information about consumer reading habits, such as the most read passages, most highlighted sections, etc. Thus, the contract between the consumer and the seller has fundamentally changed, so that reading is no longer just a personal experience, but also includes the sharing of data about when a consumer accesses the book and what she likes the most[2]. The possibility that the seller of a digital good could obtain additional information throughout the product's life span should, in our opinion, play a role in customers' purchasing decisions, specifically, via privacy uncertainty.

As physical and digital goods differ in their privacy implications, we must evaluate new privacy needs of consumers as they interact with digital goods and investigate how the absence of disclosure regarding information practices of the seller causes privacy uncertainty. Consumers are known to be poor decision makers about revealing their personal information and there have been calls to understand how privacy uncertainty can arise (Acquisti and Grossklags 2008). However, to date, no comprehensive work has been undertaken on this dimension of uncertainty in online transactions. Although Belanger and Crossler (2011) and Smith et al. (2011), in their extensive literature reviews, note the need to inform consumers about data disclosure when buying online, thus far, the research has been limited to understanding the broader role of privacy concerns. Instead, we argue that it should go beyond such concerns during the sales transaction to uncover underlying privacy uncertainties during the life cycle of digital goods. Consequently, our work is novel as we highlight this little-known yet vital phenomenon, which will improve our theoretical understanding of privacy uncertainty and guide best practices on how to handle consumers' personal information.

3 Privacy Uncertainty in the Mobile Apps Market

[2] http://www.theatlantic.com/technology/archive/2014/11/the-passages-that-readers-love/381373/

In this section, we develop a theoretical model to explain the role and origin of privacy uncertainty. First, we establish the concept of privacy uncertainty and then discuss its antecedents in the form of the information asymmetry that arises in the context of mobile apps. Finally, we explore the impact of privacy uncertainty on willingness to buy a mobile app along with that of product and seller uncertainties and other control variables in the mobile apps market.

3.1 Privacy Uncertainty

While physical products are commonly sold online and technologies are in place to accommodate these sales, the Internet also facilitates the provision of digital goods such as platforms (e.g., Facebook, Twitter, search engines), portals (e.g., Yahoo), news sites (e.g., nytimes.com, Huffington Post), and independent software applications (e.g., apps on Facebook or smartphones). The distinction between these digital goods, particularly new apps, and physical goods is that the former rely on a continuous interaction between the consumer and the seller's platform. While some of these software products or services are purchased, most are free. Consumers "pay" for these digital goods by sharing their personal information and usage patterns. These two components (personal information and usage patterns) can be combined to develop profiles of consumers and can therefore be used to offer personalized advertisements. Thus, customers' behavior and information become part of an ongoing transaction, which only terminates when the app is removed from the mobile device.

Consequently, when consumers consider buying these products, they should also be interested in determining how the seller utilizes their personal information over time. To understand this phenomenon, we focus on mobile apps, since they are among the most popular digital products. Apps can be free or sold for a price. Almost all require some personal information that is used within the app or for other purposes, such as providing behavioral advertisements to their users. When users are prompted to share information, they need to decide how this will affect their privacy. In many cases, they may not even be asked to disclose any data, but their content and usage patterns are automatically shared with the seller. In

other words, consumers confront a decision regarding the privacy of their information when they choose to download an app and experience (privacy) uncertainty in the absence of relevant information.

Consistent with Dimoka et al. (2012), our definition of uncertainty conforms to Knightian uncertainty (Knight 1921), which arises from *imperfect* information. That is, individuals usually have no clear way to estimate the likelihood and consequences of privacy breaches (Acquisti and Grossklags 2005; Acquisti and Grossklags 2008). In the absence of accurate information, they will be unable to predict their future privacy state, resulting in *privacy uncertainty,* which is defined *as the buyer's difficulty in assessing the privacy of the information accessed and acquired by the app.*

A closely related concept is *privacy risk*, or an "individual's calculation of likelihood of negative outcomes" from sharing information (Dinev et al. 2012; Xu et al. 2011). This construct is derived from psychological risk literature, which focuses on how subjects form their risk beliefs and whether their perception is consistent with the actual risk (Guseva and Rona-Tas 2001; Leroy and Singell 2013). Since negative risk perceptions are usually heightened (Kahneman and Tversky 1979; Tversky and Fox 1995; Tversky and Kahneman 1991), the thrust of this literature is only on negative dimension of risk. As privacy uncertainty draws on concepts of seller uncertainty and product uncertainty (Dimoka and Pavlou 2008; Dimoka et al. 2012; Hong and Pavlou 2014), the focus of the current study is on the perception of uncertainty in predicting the quality of the seller, the product, or one's privacy in the absence of information. Thus privacy risk and privacy uncertainty emerge from two separate research streams and should not be conflated. Whereas privacy risk is associated with negative perceptions of data sharing, privacy uncertainty relates to consumers' *inability* to evaluate privacy risk due to imperfect information. In essence, privacy uncertainty encompasses the full spectrum of negative and positive perceptions that arise from information asymmetry. Moreover, when considering privacy uncertainty, we are not concerned whether consumers experience psychological risk, but rather whether they can make an accurate assessment of their privacy risk.

3.2 What Drives Privacy Uncertainty?

In an economic transaction, uncertainty arises when the seller has more information about a product than the buyer does (Knight 1921; Akerlof 1970). The difference in information between transacting parties is often referred to as information asymmetry (Mishra et al. 1998). Information asymmetry can exist during pre-purchase and post-purchase phases. In the former, the consumer has asymmetric information about attributes of the product that concern her before the sale, and in the latter, she has asymmetric information about its post-purchase use.

Within the context of mobile apps, consumers face both pre- and post-purchase information asymmetry. Figure 1 summarizes our conceptual model, where we distinguish between asymmetry types and their dimensions. For pre-purchase information asymmetry, we consider *hidden information*, whereas for post-purchase asymmetry, we consider *hidden action* and *hidden effort*. Any information asymmetry arises due to consumers' imperfect information about how the mobile app manages their data. In particular, consumers need to know about three aspects of their personal information management: collection, use, and protection. These dimensions are consistently cited in the privacy literature (Malhotra et al. 2004; Smith et al. 1996; Xu et al. 2012) and promoted by the Federal Trade Commission (FTC) as the aspects of privacy that sellers must consider if they wish to offer better privacy services to their consumers.

To understand the antecedents, we need to analyze a consumer's privacy information needs in mobile app purchases, as summarized in Table 2. Almost all mobile apps collect and use some personal information, either to enhance their operation and capability, or to deliver targeted ads. Moreover, in most cases, the information is passed to the app seller and/or app store, such as Apple or Google. The data is usually stored on the app seller's servers, which are managed by the app seller or are rented. Occasionally, it is given to third-party information aggregators that may be located in other countries.

Figure 1: Theoretical Model for Information Asymmetry and Its Effects on Privacy Uncertainty

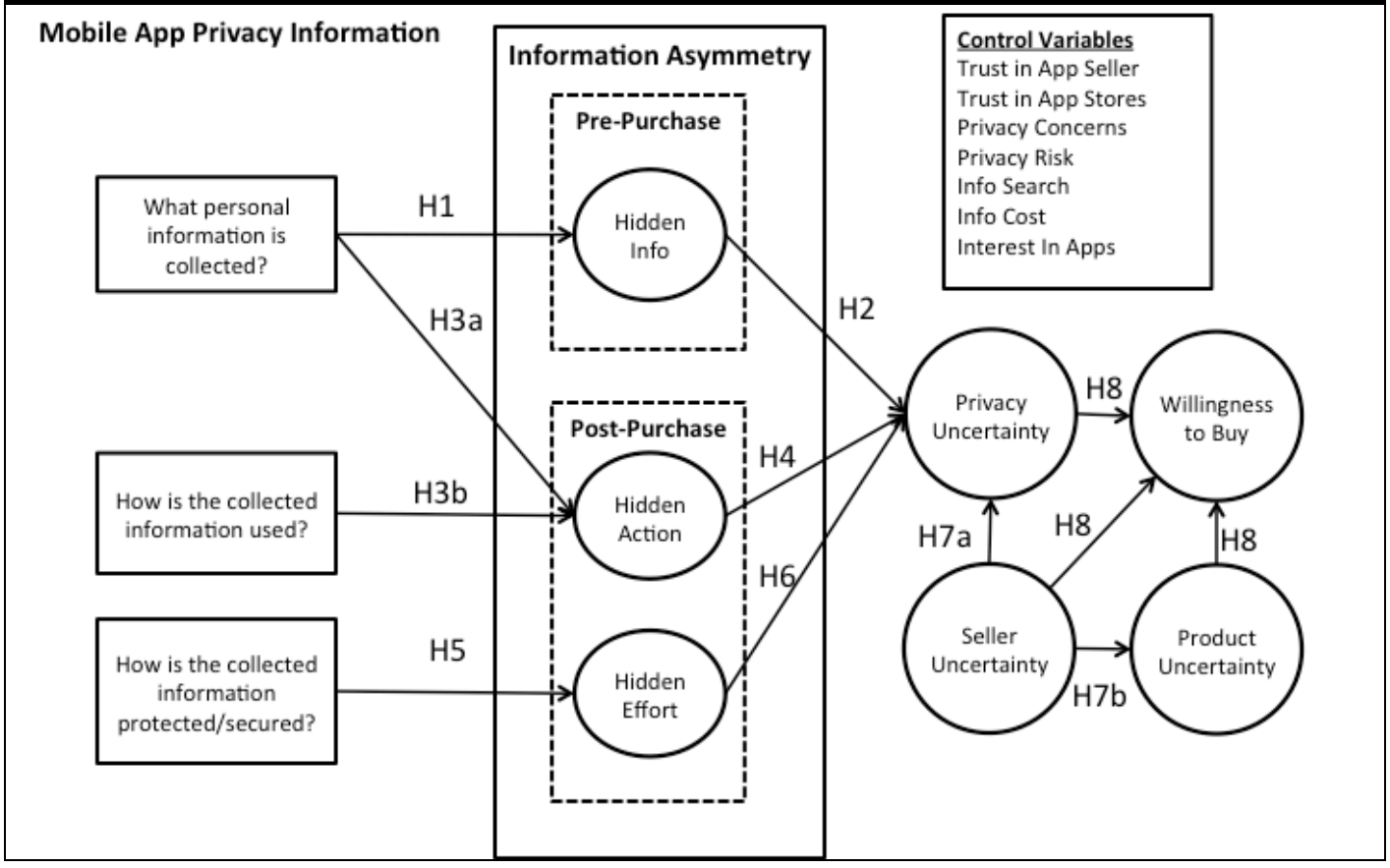


Table 2: Privacy Information Needs of Consumers when Purchasing Mobile Apps		
Privacy Information*	**Description**	**Nature and Effects**
Collection of Information: At the time of purchase, whether the seller collects information that is relevant to the app's functionality.	Most mobile apps request some personal information from the consumer. It may be used to improve functionality; for instance, a mapping service will require access to the global positioning system (GPS) on the user's mobile phone to show her current location on a map. Similarly, most apps require additional information, such as name, age, and gender, to personalize the experience.	**Nature:** Pre- and Post-Purchase Information **Effects:** Hidden Information and Hidden Action
Use of Collected Information: After the purchase, whether the information collected will be used as claimed by the app seller.	While apps may gather personal data for the purpose of personalization, vendors derive additional revenue by selling it and/or providing behavioral advertisements. Thus, a consumer wants to know how the seller intends to use the collected information. This can help her gauge whether such use of the information is appropriate and whether she is comfortable with the seller's policies. Therefore, if no information is available on what the seller will do with the collected information, the consumer has no way to determine whether it will be employed only within the app, used to provide advertisements, or sold to a third party. This creates information asymmetry about the app seller's future intentions.	**Nature:** Post-Purchase Information **Effects:** Hidden Action
Protection of Collected Information: After the purchase, whether the seller has appropriate privacy practices (e.g., firewall, encryption) to protect consumers' information from malicious use.	When the consumer discloses her information during a sale, the app seller becomes a co-owner of this information. In addition, the information is physically stored on the app seller's hardware (servers). It is now up to the app seller to protect this data so that it does not get into the hands of a malicious entity who exploits it to harm the owner (consumer). An app seller may or may not invest in the appropriate hardware and make an effort to protect buyers' information. Thus, the consumer wants to know what security practices the app seller has adopted.	**Nature:** Post-Purchase Information **Effects:** Hidden Effort
*These three dimensions are consistently referenced in the privacy literature (Malhotra et al. 2004; Smith et al. 1996; Xu et al. 2012) and promoted by the Federal Trade Commission (FTC) as the aspects of privacy that sellers must consider if they wish to offer better privacy services to their consumers.		

Uncertainty occurs because the buyer may not know what personal information is collected. In addition, once the app is purchased, she may be unaware of how the data will be used or whether it will be protected. The app seller can choose to abide by industry norms or to break its promises by passing the data on to information aggregators. In addition, there is the chance of the app seller's servers being hacked by a malicious user and the buyer's personal information being stolen as a consequence (e.g., Sony, LinkedIn, and Target). If the information asymmetry cannot be reduced, consumers will become uncertain (Arrow 1963). In the case of mobile apps, they may doubt the quality of the privacy of their information entrusted to the app.

In the next section, we relate consumers' privacy information needs with information asymmetry, more specifically, with how the absence of information about a certain dimension of privacy practices of an app seller causes an information asymmetry between transacting parties, both before and after the sale. Before deciding to buy the app, the consumer tries to determine whether her knowledge about personal information collection is complete (i.e., she knows exactly what information the app will collect) and to interpret whether the seller will continue to honor its claims regarding how her information is used and protected after the purchase.

3.3 Pre-Purchase Information Asymmetry in Privacy

3.3.1 Hidden Information

Hidden information is defined as *the consumer's perception that app seller has more knowledge of what personal information about the consumer is being collected by the app but do not fully report this information to the consumer*. A key aspect of hidden information is that it is pre-contractual (Akerlof 1970). The concept has been applied to bank loans (De Meza 2002; Nash and Sinkey 1997) and health insurance (Doherty and Thistle 1996). Before the actual transaction takes place, the principal party must ascertain whether the agent is presenting complete information. For instance, when deciding to lend money, the bank is interested in whether the loan seeker has a good financial standing. Similarly, an insurer would like to know whether a person seeking health insurance has any preexisting conditions that

should be brought into the contract. In both cases, the lack of information about the other party leads to a perception that it is hiding essential facts about certain characteristics. In an online context, this could be the absence of descriptive information about a product (Dimoka et al. 2012). This lack of information may reflect the seller's technical inability to provide a description on the website or, alternatively, a malicious intent to defraud the customer.

In the context of mobile apps, the crucial data is a list of all the personal information that is collected. At the time of purchase, a seller can easily disclose this, as the seller is always better informed than the consumer. If the app seller does not provide any details about what information is being collected and the customer notices its absence, then she will perceive information asymmetry.

> ***Hypothesis 1:*** *A consumer's perception of hidden information will be heightened when she cannot find information about the information collection practices of a mobile app.*

This perceived information asymmetry will cause the consumer to become unsure about the privacy of the personal information that the app can obtain, since she cannot tell whether the app seller is withholding information due to negligence or malicious intent. While most collected information is presumably either required for the functioning of the app or used to enhance its capability, apps can also gather facts that they do not necessarily need (e.g., the location information accessed by a standalone gaming app is not required for its operation). If, at the time of purchase, the consumer understands what personal information is being collected by the app now or later, she can determine more easily whether the data accessed by the app is relevant or potentially intrusive. However, a heightened perception of hidden information will increase uncertainty about what data the app uses and whether it is relevant to its operation (Dimoka and Pavlou 2008; Dimoka et al. 2012; Pavlou et al. 2007).

Thus, if a consumer thinks that the seller is hiding something about the personal information being collected, she will be less certain about personal privacy. Consistent with the literature arguing that the consumer experiences uncertainty when she perceives that the seller is hiding information, we contend

that a consumer's privacy uncertainty increases if she believes the seller is obfuscating its information collection practices.

> ***Hypothesis 2:*** *A high level of perceived hidden information will increase privacy uncertainty.*

3.4 Post-Purchase Information Asymmetry in Privacy

Since hidden action and hidden effort are post-purchase phenomena, we focus on the information needs at the time of purchase of the principal party (i.e., the consumer) regarding how the app seller will use and protect her information once the purchase has been made. Thus, the consumer will fear that the seller may renege on its privacy claims and compromise her personal information by either misusing it or not protecting it. We first discuss hidden action, followed by hidden effort in the following subsections.

3.4.1 Hidden Action (Fear of Seller Opportunism)

In the mobile apps context, hidden action is *the consumer's perception that, given a profitable opportunity, app sellers may not act according to their claims and guidelines concerning information use*. Hidden action is a post-purchase issue (Rothschild and Stiglitz 1992) in which the consumer believes that sellers "need an incentive to act obediently according to the plan" (Myerson 2013). In marketing, this phenomenon is described as "fear of seller opportunism," that is, if given a chance, the seller may take advantage of the consumer's inability to determine its post-purchase actions (Mishra et al. 1998; Pavlou et al. 2007).

With regards to hidden action in the context of privacy, information collection and use are of concern. If a consumer perceives that the collection of certain information is being hidden, then she may feel that the seller has ill intentions for the use of the data. Since information use is related to how the app utilizes a consumer's personal content after it has been collected, we would expect these two types of app seller's information practices to affect hidden action.

> ***Hypothesis 3a:*** *A consumer's perception of hidden action will be heightened when she cannot find information about the data collected by a mobile app.*

Hypothesis 3b: *A consumer's perception of hidden action will be heightened when she cannot discover how the mobile app seller will use the collected information.*

We expect an increase in hidden action to lead the consumer to have high privacy uncertainty. This is primarily because if the buyer cannot be sure how the seller will behave in the future, she will have *difficulty in assessing* how her privacy will fare. This is parallel to online transactions for physical goods, where in the absence of information regarding the seller's post-purchase behavior, the consumer cannot determine whether it will actually ship the product (Pavlou et al. 2007). Similarly, in the context of mobile apps, while the app seller may or may not misbehave in the future, having no information about its post-purchase behavior will induce privacy uncertainty.

Hypothesis 4: *A high level of perceived hidden action will increase privacy uncertainty.*

3.4.2 Hidden Effort

Hidden effort is another post-purchase information asymmetry (Myerson 2013) and defined as *the consumer's perception that an app seller may not spend enough effort to protect consumer's privacy*. When we consider hidden action, we refer to an app seller's self-serving intent, whereas when we consider hidden effort, we are concerned about whether it will protect the consumer's information appropriately. What distinguishes hidden effort from hidden action is in the intention, i.e., whether or not the agent is diligent enough to do a good job. For instance, in the case of car insurance, while a person may drive carefully, she may not take care of the car as intended, e.g., not change the oil on time or have appropriate tire pressure (Chiappori et al. 2006). Moreover, hidden effort is a prominent source of information asymmetry in contracts related to outsourcing, where the party that outsources the job cannot determine whether the subcontractor is working diligently (Barthelemy 2001). Similarly, the issue of hidden effort arises for companies using skilled labor to manufacture products (Porteus and Whang 1991). Here, the employer cannot determine whether workers are performing to the best of their abilities. In essence, the employer lacks direct information on the quality of the effort the worker exerts in doing his job.

Hidden effort has not been discussed in the prior information systems literature, which has focused on whether a consumer can determine the quality of a product sold online and whether the seller will then meet its contractual obligations. However, in the context of privacy, the consumer also tries to determine if the seller will protect his or her personal information diligently in an ongoing fashion. Since the consumer does not know how privacy conscious the seller will actually be, the lack of information about data protection practices may lead her to be uncertain about whether the seller will actively protect her privacy.

> ***Hypothesis 5:*** *A consumer's perception of hidden effort will be heightened when she cannot tell how the mobile app seller will protect the collected information.*

If the seller does not disclose how it will protect the collected information and the consumer perceives that it is hiding information about its ongoing privacy efforts, she will have difficulty in determining whether it will store and protect her data appropriately. Since the consumer experiences a high level of perceived hidden effort, she may fear that the seller is lax and does not care about protecting information, allowing it to be accessed easily by malicious users. Thus, consistent with the prior findings that a party experiences uncertainty when she thinks that the other party is hiding information about its effort (Barthelemy 2001; Chiappori et al. 2006; Porteus and Whang 1991), we contend that if the consumer feels that she cannot determine whether the seller will exert appropriate effort in protecting information privacy, she will have higher privacy uncertainty.

> ***Hypothesis 6:*** *A high level of perceived hidden effort increases privacy uncertainty.*

3.5 Nomological Relationship of Privacy Uncertainty with Seller and Product Uncertainty

A consumer contemplating to buy an app also confronts product and seller uncertainty. Since the seller usually develops the app and can compare it to similar ones in the market, he knows more about its quality and capability than the purchaser. This knowledge difference leads to asymmetric information, which in turn, creates uncertainty for the buyer. In the context of buying a used car online, in which the

buyer must evaluate many physical features to assess the car's quality, Dimoka et al. (2012) theorize product uncertainty as relating to many aspects of the car's condition, such as the shape of the wheels and the timing belt (performance uncertainty) and how those aspects are represented on the e-commerce platform (description uncertainty). Unlike used cars whose product quality is influenced by multitude of factors and conditions, mobile apps are less complicated. Product quality in the context of a mobile app is characterized in relations to the user's experience in using the app. Consequently; we consider product uncertainty as *the buyer's difficulty in assessing the quality of the mobile app*.

Seller uncertainty is closely related to product uncertainty. For mobile apps, seller uncertainty relates to the core competencies of the seller, that is, the seller's capability will determine how well the app is developed. Therefore, seller uncertainty is defined as *the buyer's difficulty in assessing the capabilities of the seller of the mobile app*. The company clearly understands its staff's programming skills and experience. Moreover, it knows whether it will continue to support the app or discontinue it at some later time. Consistent with the prior literature (Dimoka et al. 2012; Gefen et al. 2003; Pavlou et al. 2007), consumers having imperfect information about the seller leads to seller uncertainty, or inability of the buyer to assess the quality of the skills of the app developer.

Since the seller develops the product, an increase in seller uncertainty also heightens product uncertainty (Dimoka et al. 2012). Similarly, since the seller developed the app that collects consumers' information, it is also responsible for using and possibly protecting information collected. If the consumer is uncertain about the capabilities of the seller, she will be unsure about whether it can appropriately manage her privacy. Thus, the uncertainty of the buyer about the seller's capabilities also increases her privacy uncertainty.

Hypothesis 7a: *For mobile apps, seller uncertainty increases privacy uncertainty.*

Hypothesis 7b: *For mobile apps, seller uncertainty increases product uncertainty.*

Lastly, we argue that, in addition to seller uncertainty (Pavlou et al. 2007) and product uncertainty (Dimoka et al. 2012), privacy uncertainty also reduces the willingness to buy. Privacy uncertainty affects

the degree to which consumers can determine the security of their information or predict the state of their privacy in the future. This future state could range from none to various levels of privacy breaches, such as information being sold to a third party leading to spamming or unwanted behavioral advertisements, or the server being hacked by malicious users leading to identity theft. Since uncertainty is a perception and consumers tend to overestimate losses (Kahneman and Tversky 1979), a high level of uncertainty will cause them to predict a high level of privacy failure. In other words, when uncertainty is high, buying an app is perceived to lead to a future state that is potentially harmful to the consumer (Pavlou et al. 2007). In such a scenario, an uncertain consumer will refrain from purchasing a mobile app.

> ***Hypothesis 8:*** *In addition to seller and product uncertainty, privacy uncertainty reduces the willingness to buy a mobile app.*

3.6 Role of Trust and Privacy Concerns

In the context of e-commerce, Pavlou et al. (2007) identify four antecedents of uncertainty: information asymmetry[3], fear of seller opportunism, trust, and privacy concerns. Of these, information asymmetry and fear of seller opportunism are derived from agency theory (Mishra et al. 1998; Pavlou et al. 2007). While all four dimensions are important in understanding uncertainty, we focus on the concepts from agency theory, notably, pre-purchase and post-purchase information asymmetry. Our rationale is twofold. First, highly competitive and fragmented apps markets make it difficult for sellers to address trust and privacy concerns. Since they are, with few exceptions, small development shops or individuals, it is not economically viable for them to invest in reputation-building exercises (e.g., developing a brand). Moreover, the economics literature also shows that in markets where competition is high and sellers are indistinguishable, trust and reputation mechanisms are not successful (Dulleck et al. 2011). Second, the existing infrastructure, which requires a platform (such as iTunes or Google Marketplace) to sell mobile apps, shields sellers from directly interacting with buyers. Thus, most app sellers only have a brief

[3] Pavlou et al. (2007) describe information asymmetry as a pre-purchase phenomenon only. However, we conform to the economics and marketing definition of information asymmetry, which describes information asymmetry as a broad phenomenon that subsumes both pre-purchase and post-purchase information asymmetry. This distinction allows us to probe further into the dimensions of information asymmetry, such as hidden information, hidden action, and hidden effort.

encounter with customers and cannot influence trust or privacy perceptions, which are deeper attitudes that form during a more holistic relationship (e.g., through a website).

While we do not explicitly theorize for the impact of trust and privacy concerns, they are used as control variables in our model and hence their effects are accounted for in our statistical analysis. Our results will show that the information asymmetry dimensions on which we focus are significant even in the presence of trust and privacy concerns.

4 Empirical Method

To test our hypotheses, we employed a factorial survey method. We recruited our respondents from Amazon Mechanical Turk and asked them to evaluate a mobile app-buying scenario.

4.1 Factorial Survey Method

A factorial survey method is a specialized version of the scenario method. In the traditional scenario method, subjects are given written descriptions of the situations before they answer the questionnaire. The scenarios are carefully crafted to focus on the message as well as its context. The scenario method has been used in information systems research, such as studies on information security policy violations (D'Arcy et al. 2009; Vance and Siponen 2012). The purpose of scenarios is to enhance realism by incorporating the relevant aspects of the context studied. Moreover, the method enforces uniformity in the situational details across all the respondents, thus reducing confounds (Alexander and Becker 1978).

While the scenario method is usually employed in surveys, it does not offer the flexibility of controlled experiments, where researchers can manipulate all the dimensions of treatment to attain an orthogonal design (Rossi 1979; Rossi and Anderson 1982; Rossi et al. 1974). The factorial survey method applies this experimental orientation to the scenario approach. It has been used extensively in sociology research (Wallander 2009) and more recently, successfully adopted by IS scholars (Vance et al. 2015).

As a hybrid of the scenario and experimental methods, the factorial survey method is enriched by the qualities of both methodologies. While the scenario method provides the richness of developing

contextual situations, the factorial method allows us to manipulate the dimensions of theoretical interest. In essence, we can build a full factorial design that encompasses all the combinations of each dimension at its different levels. This gives us different treatment groups, ensures an orthogonal design, and reduces the problem of multicollinearity (Jasso 2006). As in the scenario method, the subjects are recruited online but are assigned randomly to different treatment groups.

4.1.1 Scenario Design

Although our research focused on the effects of information about privacy practices of the app seller on privacy uncertainty, we did not wish to prime our subjects with the privacy context. Also, to test our hypotheses, we wanted subjects to make their decisions in a regular mobile app-purchasing setting. While the most realistic setting would be the actual platforms where mobile apps are sold, those platforms neither are available for research nor provide the flexibility to measure subjective responses. Thus, we attempted to develop realistic mobile app-buying scenarios by replicating the online app store experience.

We created a profile of a fictitious gaming app that resembled an app on a typical app store. This profile of a fictitious gaming app consisted of all the relevant information potentially used to make an app buying decision. We used a gaming app since games are the most popular category of apps and it is known that they collect users' personal information. Since most of these apps do not include explicit privacy notices, we incorporated information about the app's privacy practices in the profile (see Figure 2). After developing screenshots of the profile of the app, we wanted to know whether subjects felt that the information they were provided with was balanced. The intent is to make sure that no single type of data in the profile dominated the others. Thus, we compared the relative importance of different information types by surveying 35 MBA students. Participants were asked to rate the value of various aspects of information and content provided in the app profile, including seller information, product information, in-game screenshots, and privacy information. We observed no significant difference in rank across these categories. Thus, on average, all the types of information (privacy, product, and seller) presented in the screenshots were considered equally important.

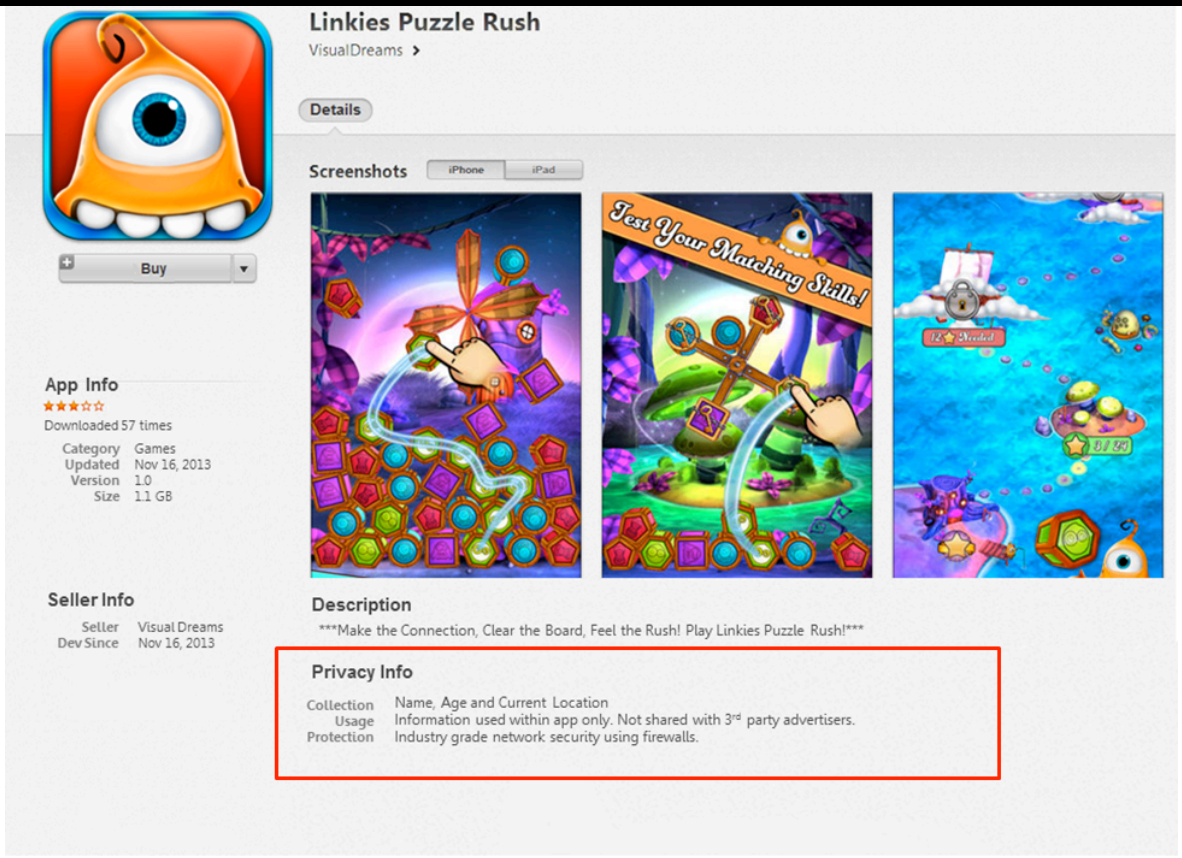
To ensure that our scenarios were realistic, at the end of the survey, we asked the participants whether they wanted more information about the app. We found that subjects believed that it was a real app and that some people even expressed an interested in buying the app.

4.1.2 Manipulations in the Factorial Survey

Since we are interested in privacy-related information asymmetry and its impact on privacy uncertainty, we focused solely on this aspect. As discussed previously, there are three types of privacy-related data in the context of mobile apps: information collection, use, and protection. Each of these data can be either present or absent from the app-buying screenshot. Consequently, we formed eight groups based on a 2 (collection) x 2 (use) x 2 (protection) combination of the presence (or absence) of these privacy information types.

Figure 2 highlights the privacy section of the screenshot, which was manipulated for the study. Note that the privacy section was not highlighted in the screenshots used in the study. The screenshot for each group has different privacy information while the rest of the profile information remained the same.

Figure 2: Screenshot of App's Profile (Showing Privacy Information Section)

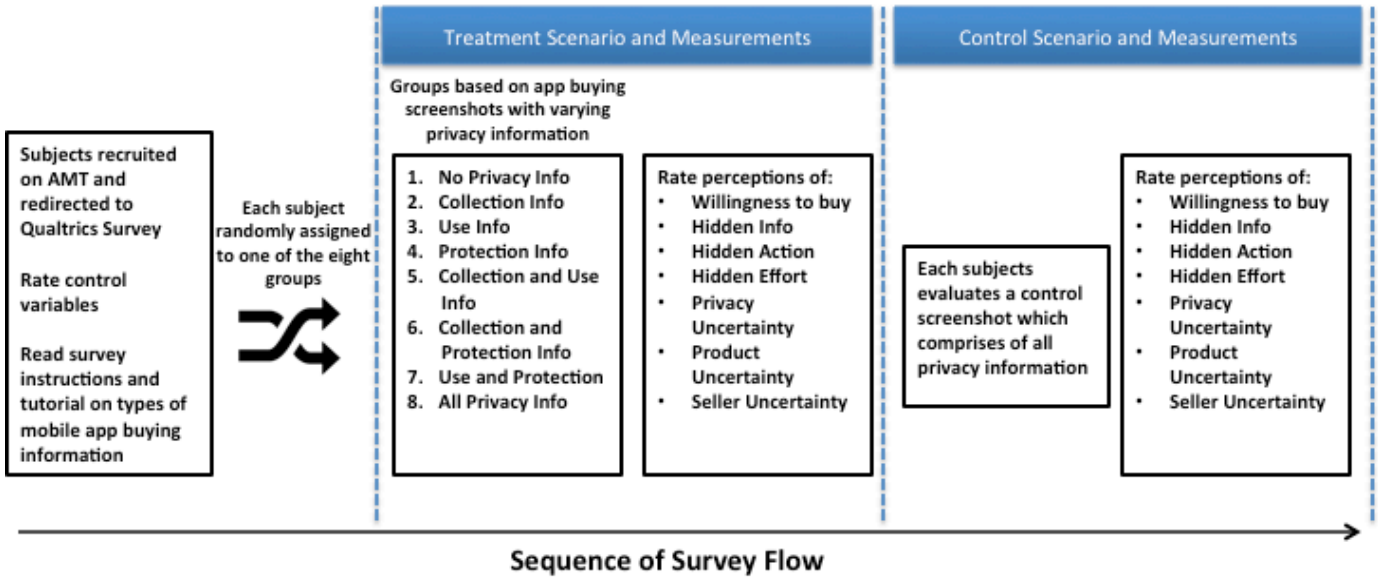


4.1.3 Study Procedure

A key challenge in designing this study is that consumers' privacy preferences are not well defined (John et al. 2011). While determining the accuracy of privacy uncertainty is an important research stream, in our experiment, we focused on the manifested privacy uncertainty. The only way subjects respond appropriately is when they are given appropriate cues before measurement (John et al. 2011). Once the subjects are appropriately cued, their preferences are stable and correlate with their privacy behavior (John et al. 2011). Thus, we showed a brief tutorial before the experiment to allow our subjects to learn "what" type of information is present and "where" on the screenshot they could find it. We took special care to avoid priming regarding the nature of the study by including information about all aspects of buying an app (seller, product, and privacy) in the tutorial.

After the tutorial, subjects were exposed to one of eight treatments, which were followed by the questions. To reduce the effect of confirmation bias, we measured willingness to buy *before* the respondents rated the uncertainty measures. Since the scenario screenshot did not contain pricing information about the app, we included it in the willingness to buy question. We set the price at $2, a common price tag for most gaming apps. At the end of the survey, subjects answered questions about other control measures, such as trust, privacy concerns, and demographics.

Figure 3: Sequence of the Survey



All subjects were recruited through Amazon Mechanical Turk. Interested participants were told that they would be participating in a study that requires them to evaluate buying scenarios of mobile apps by reading different aspects of mobile apps, such as product, seller and privacy information. Once they decided to participate, they were taken to the Qualtrics website, where the survey was hosted. Figure 3 outlines the survey flow. First, the subjects filled in the consent form, which was followed by questions related to trust, privacy concerns, and mobile app-buying behavior (i.e., control variables). We measured

trust and privacy concerns because they have been theoretically proposed as antecedents of privacy uncertainty (Pavlou and Fygenson 2006). Moreover, marketing literature shows that consumers information seeking behavior is influenced by their interest in the product and their general information seeking behavior (Brucks 1985; Urbany et al. 1989). Thus we also measured how much time subjects spend on reading privacy information (Info Search), whether subjects felt that they were efficient in their information search (Search Cost) and finally whether subjects regularly buy mobile gaming apps (Interest in App). Then, subjects went through a tutorial to familiarize themselves with the information types and where they were located on the screenshots. Afterwards, each subject was randomly assigned to one of the eight treatment groups. He or she was offered the corresponding information associated with the treatment and then asked to rate all the dependent variables. This was followed by a control scenario containing *all* three information elements (collection, use, protection), in which subjects rated the dependent variables again. For instance, if a subject is assigned to a treatment where information about use and protection is provided but not information about collection, she will see all three types of information in the control scenario. The difference between treatment and control scenarios allows us to measure the effect of the *presence* of a particular kind of information when it is added to subjects' consideration set. In addition, the control scenario provides us with a base condition against which subject's perceptual differences can be accurately measured. Since subjective responses are relative to the "prevailing norm or adaptation level", it is important for subjects to be able to compare treatments relative to each other (Helson 1964). This practice is also consistent with other information system studies (Jiang & Benbasat, 2004; Kim & Benbasat, 2006; Lim & Benbasat, 2000).

As an alternative design, we could have had subjects first rate the full information scenario (i.e., control scenario) and then the treatment. However, in that case, they would have experienced a "loss" in information. Since subjects overweigh the effect of losses compared to that of gains (Kahneman and Tversky 1979; Tversky and Fox 1995), we chose a conservative approach wherein the control scenario was shown after the treatment scenario to create a gain condition. Thus, if our results hold in the gain

condition, they will also hold in the loss condition. Finally, we performed a manipulation check to determine whether subjects realized which information was missing in the treatment scenario.

4.1.4 Data

The use of online panels is becoming increasingly popular in information systems research because of the quality of the participants and their responses (Lowry et al. 2013; Lowry et al. 2015; Posey et al. 2013). We therefore turned to Amazon Mechanical Turk (AMT) to recruit our respondents. Researchers have found no difference between the results of cognitive experiments conducted in the lab and those conducted on AMT (Crump et al. 2013). Moreover, AMT allows us to access people of diverse ages and backgrounds. In addition, since the participants do not have to come to a physical lab and respond under observation, its use reduces confirmation bias.

We recruited 187 U.S.-based participants from AMT, of which 180 completed the study and were retained for analysis. Among the participants, 51% were female. All were between ages 18 and 55 and owned smartphones. Each participant was randomly assigned to one of the eight groups. On average, people spent 12 minutes completing the study.

5 Conclusion

We set out to define privacy uncertainty and to show its presence in a nomological network of constructs that includes seller uncertainty and product uncertainty. In addition, we delved deeper into the concept to determine its antecedents. We hypothesized that two different classes of information asymmetry lead to privacy uncertainty. Using a simulated mobile app-buying experiment, we found that privacy uncertainty is indeed a statistically significant construct. Moreover, our results show that post-purchase information asymmetry matters more to consumers than pre-purchase information asymmetry.

Theoretically, we extended the uncertainty research in information systems and introduced privacy uncertainty as an independent construct. In addition, we discovered that within the ambit of post-purchase information asymmetry, hidden action is a dominant factor. This result has important implications for app

sellers. For instance, while the "notice and consent" mechanism allows users to determine what information is being collected, it does not explain how the seller will actually utilize it.

A few limitations of this study also provide opportunities for future research. Firstly, due to the nature of our controlled experiment, the generalizability of this research is suspect. In addition, while we control for aspects of seller and product information, the online market contains heterogeneous products, which means that our findings may not apply in the broader mobile app context. Therefore, future researchers can test this theory in a more generalizable fashion, where the effects of privacy and other uncertainties can be measured for different types of applications and preferably at different price points.

Secondly, our operationalization heightens consumers' understanding of privacy when purchasing mobile apps. However, customers may not be as aware in real-world scenarios, which involve buying apps on small-screen mobile phones in a short time frame. To theorize this uncertainty, consumers must show stable preferences. However, if their preferences are not stable, they may perceive greater or lesser uncertainty regardless of the situation. This is true when consumers are unfamiliar with a decision-making process (Bloch et al. 2014; Jeffrey and Richard 1996). Thus, an immediate extension of this work would relate to measurement and bias in the assessment of consumers' privacy uncertainty. If consumers perceive uncertainty accurately, they will seek information to reduce it and will consequently find the best products. However, if they perceive uncertainty inaccurately, their choices will not reflect their actual preferences. This also hinders sellers from introducing privacy features, as consumers will not be able to appreciate them.

References

Acquisti, A., and Grossklags, J. 2005. "Privacy and Rationality in Decision Making," *IEEE Security and Privacy* (3:1), pp. 24–30.

Acquisti, A., and Grossklags, J. 2008. "What Can Behavioral Economics Teach Us About Privacy?" *Digital Privacy: Theory, Technologies, and Practices*, S. De Capitani di Vimercati, S. Gritzalis, C. Lambrinoudakis, and A. Acquisti (eds.), Boca Raton, FL: Auerbach Publications, pp. 363–377.

Akerlof, G. A. 1970. "The Market for Lemons : Quality Uncertainty and the Market Mechanism," *The Quarterly Journal of Economics* (84:3), pp. 488–500.

Alexander, C. S., and Becker, H. J. 1978. "The Use of Vignettes in Survey Research," *Public Opinion Quarterly* (42:1), pp. 93–104.
Andersson, L. M., and Bateman, T. S. 1997. "Cynicism in the Workplace: Some Causes and Effects," *Journal of Organizational Behavior* (18:5), pp. 449–469.
Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), p. 32.
Arrow, K. J. 1963. "Uncertainty and the Welfare Economics of Medical Care," *The American Economic Review* (53:5), pp. 941–973.
Barthelemy, J. 2001. "The Hidden Costs of It Outsourcing," *MIT Sloan Management Review* (42:3), p. 60.
Belanger, F., and Crossler, R. E. 2011. "Theory and Review Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017–1041.
Bloch, P. H., Sherrell, D. L., and Ridgway, N. M. 2014. "Consumer Search : An Extended Framework," *Journal of Consumer Research* (13:1), pp. 119–126.
Brucks, M. 1985. "The Effects of Product Class Knowledge on Information Search Behavior," *Journal of Consumer Research*), pp. 1-16.
Buck, D.-K. C., Horbel, C., Kessler, T., and Christian, C. 2014. "Mobile Consumer Apps: Big Data Brother Is Watching You," *Marketing Review St. Gallen* (31:1), pp. 26–35.
Chatterjee, S., and Datta, P. 2008. "Examining Inefficiencies and Consumer Uncertainty in E-Commerce," *Communications of the Association for Information Systems* (22:1), p. 29.
Chiappori, P. A., Jullien, B., Salanié, B., and Salanié, F. 2006. "Asymmetric Information in Insurance: General Testable Implications," *RAND Journal of Economics* (37:4), pp. 783–798.
Crump, M. J., McDonnell, J. V., and Gureckis, T. M. 2013. "Evaluating Amazon's Mechanical Turk as a Tool for Experimental Behavioral Research," *PloS one* (8:3), p. e57410.
D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98.
De Meza, D. 2002. "Overlending?" *The Economic Journal* (112:477), pp. F17–F31.
Dellarocas, C. 2003. "The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms," *Management Science* (49:10), pp. 1407–1424.
Dimoka, A., and Pavlou, P. 2008. "Industry Studies Association Working Paper Series: Understanding and Mitigating Product Uncertainty in Online Auction Marketplaces,").
Dimoka, A., Hong, Y., and Pavlou, P. A. 2012. "On Product Uncertainty in Online Markets: Theory and Evidence," *MIS Quarterly* (36:2), pp. 395–A315.
Dinev, T., Xu, H., Smith, H. J., and Hart, P. 2012. "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts," *European Journal of Information Systems* (22:3), pp. 295–316.
Doherty, N. A., and Thistle, P. D. 1996. "Adverse Selection with Endogenous Information in Insurance Markets," *Journal of Public Economics* (63:1), pp. 83–102.
Dulleck, U., Kerschbamer, R., and Sutter, M. 2011. "The Economics of Credence Goods: An Experiment on the Role of Liability, Verifiability, Reputation, and Competition," *American Economic Review* (101:2), pp. 526–555.
Featherman, M. S., and Pavlou, P. A. 2003. "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human-Computer Studies* (59:4), pp. 451–474.
Franklin, J., Perrig, A., Paxson, V., and Savage, S. 2007. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants," *ACM conference on Computer and Communications Security*, pp. 375–388.
Gantz, J., and Reinsel, D. 2012. "The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East," *IDC iView: IDC Analyze the Future* (2007), pp. 1–16.
Gefen, D., Karahanna, E., and Straub, D. W. 2003. "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly* (27:1), pp. 51–90.

Gefen, D., and Straub, D. 2005. "A Practical Guide to Factorial Validity Using Pls-Graph: Tutorial and Annotated Example," *Communications of the Association for Information Systems* (16:1), p. 5.
Gefen, D., Straub, D., and Boudreau, M.-C. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the Association for Information Systems* (4:1), p. 7.
Ghose, A. 2009. "Internet Exchanges for Used Goods: An Empirical Analysis of Trade Patterns and Adverse Selection," *MIS Quarterly* (33:2), pp. 263–291.
Guseva, A., and Rona-Tas, A. 2001. "Uncertainty, Risk, and Trust: Russian and American Credit Card Markets Compared," *American Sociological Review* (66:5), pp. 623–646.
Hair, J. F., Anderson, R. E., Tatham, R. L., and William, C. 1998. "Black (1998), Multivariate Data Analysis,").
Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., and Png, I. P. L. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp. 13–42.
Helson, Harry. (1964). Adaptation-level theory.
Hölmstrom, B. 1979. "Moral Hazard and Observability," *Bell Journal of Economics* (10:1), pp. 74–91.
Holt, T. J. 2007. "Subcultural Evolution? Examining the Influence of on-and Off-Line Experiences on Deviant Subcultures," *Deviant Behavior* (28:2), pp. 171–198.
Holt, T. J., and Graves, D. 2007. "A Qualitative Analysis of Advance Fee Fraud Email Schemes," *International Journal of Cyber Criminology* (1), pp. 137–154.
Hong, Y., and Pavlou, P. A. 2010, May 5. "Fit Does Matter! An Empirical Study on Product Fit Uncertainty in Online Marketplaces," *Working Paper*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600523.
Hong, Y., and Pavlou, P. A. 2014. "Product Fit Uncertainty in Online Markets: Nature, Effects, and Antecedents," *Information Systems Research* (25), February 2015, pp. 328–344.
Hui, K. L., Teo, H. H., and Lee, S. Y. T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31:1), pp. 19–33.
James, L. 2005. *Phishing Exposed*, Rockland, MA: Syngress.
Jarvenpaa, S. L., and Staples, D. S. 2000. "The Use of Collaborative Electronic Media for Information Sharing: An Exploratory Study of Determinants," *Journal of Strategic Information Systems* (9:2), pp. 129–154.
Jasso, G. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments," *Sociological Methods & Research* (34:3), pp. 334–423.
Jeffrey, B., and Richard, A. 1996. "A Proposed Model of External Consumer Information Search,").
Jiang, Z., and Benbasat, I. 2004. "Virtual Product Experience: Effects of Visual and Functional Control of Products on Perceived Diagnosticity and Flow in Electronic Shopping," *Journal of Management Information Systems* (21:3), pp. 111–147.
John, L. K., Acquisti, A., and Loewenstein, G. 2011. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research* (37:5), pp. 858–873.
Kahneman, D., and Tversky, A. 1979. "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* (42:2), pp. 263–291.
Kiel, G.C., and Layton, R.A. 1981. "Dimensions of Consumer Information Seeking Behavior," *Journal of Marketing Research*), pp. 233-239.
Kim, Dongmin, & Benbasat, Izak. (2006). The effects of trust-assuring arguments on consumer trust in Internet stores: Application of Toulmin's model of argumentation. *Information Systems Research, 17*(3), 286--300.
Kirmani, A., and Rao, A. R. 2000. "No Pain, No Gain: A Critical Review of the Literature on Signaling Unobservable Product Quality," *Journal of Marketing* 66:2), pp. 66–79.
Knight, F. H. 1921. *Risk, Uncertainty and Product*, New York: Hart, Schaffner and Marx.

Leroy, S. F., and Singell, L. D. 2013. "Knight on Risk and Uncertainty," *Journal of Political Economy* (95:2), pp. 394–406.
Lim, Kai H., & Benbasat, Izak. (2000). The effect of multimedia on perceived equivocality and perceived usefulness of information systems. *MIS Quarterly*, 449--471.
Lowry, P. B., Moody, G. D., Galletta, D. F., and Vance, A. 2013. "The Drivers in the Use of Online Whistle-Blowing Reporting Systems," *Journal of Management Information Systems* (30:1), pp. 153–190.
Lowry, P. B., Posey, C., Bennett, R. B. J., and Roberts, T. L. 2015. "Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust," *Information Systems Journal* (25:3), pp. 193–273.
Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336–355.
Meeker, M., and Wu, L. 2013. "Kpcb Internet Trends 2013," *Internet Trends D11 Conference*.
Mishra, D. P., Heide, J. A. N. B., and Cort, S. G. 1998. "Information Asymmetry Agency and Levels of Relationships," *Journal of Marketing Research* (35), pp. 277–295.
Moore, G. C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), pp. 192–222.
Myerson, R. B. 2013. *Game Theory*, Boston: Harvard University Press.
Nash, R. C., and Sinkey, J. F. 1997. "On Competition, Risk, and Hidden Assets in the Market for Bank Credit Cards," *Journal of Banking & Finance* (21:1), pp. 89–112.
Nelson, P. 1970. "Information and Consumer Behavior," *Journal of Political Economy* (78:2), pp. 311–329.
Newman, G. R., and Clarke, R. V. 2013. *Superhighway Robbery*, New York: Routledge.
Nunnally, J. C., and Bernstein, I. H. 1967. *Psychometric Theory,* New York: McGraw-Hill.
Pavlou, P., and Fygenson, M. 2006. "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly* (30:1), pp. 115–143.
Pavlou, P., and Gefen, D. 2004. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15), pp. 37–59.
Pavlou, P. A., Liang, H. G., and Xue, Y. J. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), pp. 105–136.
Peppet, S. R. 2011. "Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future," *Nw. UL Rev.* (105), p. 1153.
Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies.," *Journal of Applied Psychology* (88:5), p. 879.
Porteus, E. L., and Whang, S. 1991. "On Manufacturing/Marketing Incentives," *Management Science* (37:9), pp. 1166–1181.
Posey, C., Roberts, T., Lowry, P. B., Bennett, B., and Courtney, J. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly* (37:4), pp. 1189–1210.
Rao, A. R., Qu, L., and Ruekert, R. W. 1997. *Brand Alliances as Information About Unobservable Product Quality*, Marketing Science Institute*, Cambridge, MA*.
Rao, A. R., Qu, L., and Ruekert, R. W. 1999. "Signaling Unobservable Product Quality through a Brand Ally," *Journal of Marketing Research* (36:2), pp. 258–268.
Rindfleisch, A., and Heide, J. B. 1997. "Transaction Cost Analysis: Past, Present, and Future Applications," *Journal of Marketing* (61:4), pp. 30–54.

Rossi, P. H. 1979. Vignette Analysis: Uncovering the Normative Structure of Complex Judgments, in *Qualitative and Quantitative Social Research: Papers in Honor of Paul F. Lazarsfeld*, R. K. Merton, J. S. Coleman, and P. H. Rossi (eds.), New York: Free Press, p. 176.
Rossi, P. H., and Anderson, A. B. 1982. "The Factorial Survey Approach: An Introduction," in *Measuring social judgments: The factorial survey approach,* P. H. Rossi and S. Nock (eds.), Beverly Hills: Sage Publications, pp. 15–67.
Rossi, P. H., Sampson, W. A., Bose, C. E., Jasso, G., and Passel, J. 1974. "Measuring Household Social Standing," *Social Science Research* (3:3), pp. 169–190.
Rothschild, M., and Stiglitz, J. 1992. *Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information*, New York: Springer.
Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989–1015.
Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), pp. 167–196.
Spiekermann, S., Grossklags, J., and Berendt, B. 2001. "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior," in *Proceedings of EC'01: Third ACM Conference on Electronic Commerce*, Tampa, FL: Association for Computing Machinery, pp. 38–47.
Taylor, R. W., Fritsch, E. J., and Liederbach, J. 2014. *Digital Crime and Digital Terrorism*, Upper Saddle River, NJ: Prentice Hall Press.
Thomas, R., and Martin, J. 2006. "The Underground Economy: Priceless," *Login: The Magazine of USENIX & SAGE* (31:6), pp. 7–16.
Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254–268.
Tversky, A., and Fox, C. R. 1995. "Weighing Risk and Uncertainty.," *Psychological Review* (102:2), pp. 269–283.
Tversky, A., and Kahneman, D. 1991. "Loss Aversion in Riskless Choice: A Reference-Dependent Model," *Quarterly Journal of Economics* (106:4), pp. 1039–1061.
Urbany, J.E., Dickson, P.R., and Wilkie, W.L. 1989. "Buyer Uncertainty and Information Search," *Journal of Consumer Research* (16:2), pp. 208-215.
Vance, A., Lowry, P. B., and Eggett, D. L. 2015. "Increasing Accountability through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *MIS Quarterly,* forthcoming.
Vance, A., and Siponen, M. T. 2012. "Is Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End User Computing* (24:1), pp. 21–41.
Wall, D. 2003. "Cybercrimes and the Internet," *Crime and the Internet*), p. 1.
Wall, D. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, MA: Polity.
Wallander, L. 2009. "25 Years of Factorial Surveys in Sociology: A Review," *Social Science Research* (38:3), pp. 505–520.
Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12), p. 798.
Xu, H., Gupta, S., Rosson, M. B., and Carroll, J. M. 2012. "Measuring Mobile Users' Concerns for Information Privacy.," *Icis*: Ftc 2009, pp. 1–16.