Journal of the Association for Information Systems

Research Paper ISSN: 1536-9323

Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem

Robert E. Crossler
Washington State University
rob.crossler@wsu.edu

Clay Posey
University of Central Florida
Clay.Posey@ucf.edu

Abstract:

Despite individuals' and organizations' best efforts, many significant information security threats exist. To alleviate these threats, researchers and policy makers have proposed new digital environments called identity ecosystems. These ecosystems would provide protection against attackers in that a third party intermediary would need to authenticate users of the ecosystem. While the additional security may help alleviate security threats, significant concern exists regarding ecosystem users' privacy. For example, the possibility of targeted attacks against the centralized identity repository, potential mismanagement of the verified credentials of millions of users, and the threat of activity monitoring and surveillance become serious privacy considerations. Thus, individuals must be willing to surrender personal privacy to a known intermediary to obtain the additional levels of protection that the proposed ecosystems suggest. We investigate the reasons why individuals would use a future identity ecosystem that exhibits such a privacy-security tradeoff. Specifically, we adopted a mixed-methods approach to elicit and assess the major factors associated with such decisions. We show that 1) intrapersonal characteristics, 2) perceptions of the controlling agent, and 3) perceptions of the system are key categories for driving intentions to use ecosystems. We found that trustworthiness of the controlling agent, perceived inconvenience, system efficacy, behavioral-based inertia, censorship attitude, and previous similar experience significantly explained variance in intentions. Interestingly, general privacy concerns failed to exhibit significant relationships with intentions in any of our use contexts. We discuss what these findings mean for research and practice and provide guidance for future research that investigates identity ecosystems and the AIS Bright ICT Initiative.

Keywords: Privacy-security Tradeoff, Trusted Identities, Information Security Ecosystem, Third Party Intermediary.

Mikko Siponen was the accepting senior editor. This paper was submitted on March 11, 2015, and went through 4 revisions.

1 Introduction

Information security is a prominent concern for many entities, such as individuals, organizations, militaries, and national governments. One core reason for such concern comes from the importance of and demand for information privacy, which represents agents' desire to have influence over data about themselves (Bélanger & Crossler, 2011). In highlighting the extent to which the protection of sensitive information is an issue, the Privacy Rights Clearinghouse has chronicled nearly 4,700 publicly reported privacy breaches in the decade from 2005-2015 in the US alone. During roughly the same time period (i.e., 2005-2014), many E.U. member countries experienced similar types of breaches with a collective total of 229 events that equated to 645 million records potentially compromised across various entities (e.g., commercial, educational, government, medical, and military) (Howard, 2014). Thus, issues surrounding the protection of sensitive data are not unique to one country, industry, or entity type.

Not surprisingly, discussions regarding the need for the development and implementation of more secure environments have arisen. The Association for Information Systems (AIS) has also recognized the need to reengineer the Internet and has launched a grand challenge called the Bright ICT Initiative (also referred to as the Bright Internet Initiative) to do so (Lee, 2015). As a result of the Bright ICT Initiative, the AIS and the United Nations International Telecommunications Union have signed a memorandum of understanding to work together to create a safe Internet that eliminates malicious attacks without sacrificing individual Internet users' privacy (Pritchett, 2015). Further outcomes of these discussions aim to improve the degree with which sensitive data are protected from threats. Interestingly, some of the more recently proposed solutions appear to offer improved security but sacrifice information privacy (Dyck & Pearson-Merkowitz, 2013; Goss, 2013; Schneier, 2008). These proposals suggest that, if online agents—individuals and organizations—are vetted and connect through a known and "trusted" identity-management intermediary, then certain types of personal information would not need to be shared across the public Internet infrastructure, which would reduce the likelihood that unknown attackers would intercept any transmitted sensitive information. Thus, agents would need to share complete and accurate identifying information with one or more known entities relatively few times (i.e., federated login) rather than known and potentially unknown entities repetitively so that agents could engage in secured activities with each other when they share sensitive data. These centralized entities would, therefore, be responsible for many activities including but not limited to vetting network agents (e.g., individual users, corporations, and educational institutions), managing credentials, and revoking access rights for agents who become noncompliant with the identity-management system specifications. Thus, researchers and policy makers have come to call these types of systems "identity ecosystems".

In summary, identity ecosystems provide a controlled environment where users provide their sensitive and identifying information to a third party that manages their and other users' access to the Internet. In doing so, users (both consumers and vendors) would not have to provide sensitive identifying information to each other to conduct secure transactions because the managing third party would have already validated them both. Conceptually, doing so would decrease the privacy and security risks in individual transactions but would necessitate users' trusting their private information to the centralized third party manager of the entire identity ecosystem. Thus, this situation creates an interesting tradeoff between selectively sharing personal information and making security-related decisions by trusting a single party with all of this information (which includes all Internet activity that one conducts in the identity ecosystem).

Various researchers and policy makers have begun to propose, develop, and implement identity ecosystems to a small degree in various countries around the world. One of the major agencies tasked with guiding such efforts in the EU is the European Network and Information Security Agency (ENISA), which acts largely in response to the European Commission COM (2012) 238. In the US, President Obama's April 2011 release of the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative is another example of a national-level initiative that aims to create a partnership between public and private entities for a more secure Internet. In fact, two U.S. states (Michigan and Pennsylvania) are currently pilot testing such an approach (Kreft, 2014), and versions of identity ecosystems have appeared in the UK in the form of the Identity Assurance Programme (d-cent, 2013). NIST suggests that the emerging use of identity ecosystems will provide a safer environment for smartphone transactions and secure business operations and will enhance public safety (NIST, 2015). Specifically, these ecosystems would provide the assurance that the Internet segment in use would be for identified users only and, hence, free—in theory—from cyber criminals and their malicious activities (Sternstein, 2011). Unfortunately, cyber protection in these ecosystems would sacrifice users' privacy rights to third parties (such as private organizations, public institutions, or a combination of both) who actually perform the

identity-verification process for all agents who want to use the ecosystem. However, to identify agents, these third parties would need to triangulate user-supplied information with other information sources such as government documents, credit reports, and any other sources they deem necessary, and serious concerns exist about the possibility of their mismanaging the security of a centralized repository that contains the verified identities of millions of ecosystem users (Gibbs, 2011). Further, some have expressed concerns that law enforcement could easily seize the stored authentication-transaction data created between a specific user and specific website without user approval (Tomhave, 2011) and other concerns that stem from "Big Brother"-type activity monitoring and surveillance (Bria et al., 2015; Whitehead, 2011). Indeed, we have recently seen debate about a country's security and an individual's privacy unfold when the U.S. Government tried to convince Apple to assist it in decrypting a domestic terrorist's iPhone (Barrett, 2016). Thus, while identity ecosystems may mean to protect the privacy of their users from one another and any potential attackers, the formation and operation of the centralized repositories necessary to run them presents significant privacy issues in and of itself.

From an academic perspective, the notion of adopting a system for improved security with so much privacy at stake is rather paradoxical. Most of the salient literature demonstrates the strong positive link between information-security efforts and information-privacy demands across myriad contexts (Bélanger, Hiller, & Smith, 2002; Buckovich, Rippen, & Rozen, 1999; Gritzalis, Kandias, Stavrou, & Mitrou, 2014; Jansen & Grance, 2011; Malhotra, Kim, & Agarwal, 2004; Miyazaki & Fernandez, 2001; Taitsman, Grimm, & Agrawal, 2013). These findings appear to contrast with the recent proposals that involve identity ecosystems in that the latter argue that effective security against unknown threats can come only at the cost of the system's users' privacy to a known intermediary. More simply, an agent's loss of privacy to a known intermediary becomes the admission price to access and conduct activities in a supposedly more secure environment that the intermediary controls. Thus, these identity ecosystems generally assume that, if the intermediary knows and "trusts" all nodes and their activities on the network, the systems enhance protection against intruders.

Given that system users generally rely on information security technologies to protect data about themselves, such identity ecosystem proposals raise an interesting research question and context that the extant literature has yet to explore:

> **RQ:** Why would individuals use a system that requires them to sacrifice their privacy on the Internet to a third party intermediary in exchange for the promise of increased security?

From a practical standpoint, we examine such a privacy-security tradeoff decision at the individual level as set forth by these ecosystems in general and the NSTIC specifically. We need to examine the factors involved in this tradeoff decision since the aforementioned E.U. and U.S. proposals call only for voluntary users. From an academic perspective, we expand the literature on the relationship between information security and privacy beyond the foundation of privacy calculus and social exchange theories by examining the context of individuals' knowingly sacrificing privacy to a trusted entity (i.e., privacy transference) in the hope they will receive improved security against additional privacy breaches by unknown entities.

Specifically, to explore these issues, we used a sequential mixed-methods approach (Venkatesh, Brown, & Bala, 2013) wherein we first elicited salient factors from transcripts that emerged from several focus group sessions. Subsequently, we quantitatively assessed these factors via structural equation modeling (SEM) using data obtained from a survey instrument. We used this approach as both a developmental and compensatory technique; that is, the quantitative analysis further developed the insight gained from qualitative focus groups and compensated for their limiting factors. As a result, we developed an initial theoretical framework to understand the factors associated with individuals' decisions to sacrifice their privacy to known intermediaries to gain increased protection against future privacy breaches.

2 Identity Ecosystems and the Privacy-security Tradeoff

Identity ecosystems are part of an overall vision of the NSTIC and other proposals for the future of a more secure Internet. Among other things, this vision promises that all agents, whether individuals or organizations, will be able to engage in online transactions with enhanced trust and security. As NIST (2015) states: "The Identity Ecosystem is a user-centric online environment, a set of technologies, policies, and agreed upon standards that securely supports transactions ranging from anonymous to fully authenticated and from low to high value". Such systems would enable individuals to use an identification card or similar device to authenticate their identity with the system, at which point the system could increase the speed of many of their transactions. No longer would individuals have to remember complicated passwords and other

login credentials because the system—managed by the third party intermediary—would already know who they are. This identification might provide further benefits, such as restricting agent access to age-appropriate content based on the individual's known attributes. The proposed system would also reduce the risk of fraud that an organization faces by providing a level of assurance that the users who make transactions are who they say they are. They would also likely enhance public safety because they could validate doctors and other professionals' certifications based on their identifying credentials.

The above examples, though by no means an exhaustive list, provide several scenarios of increased security in both the virtual and physical realms that identity ecosystems could potentially achieve. Despite these potential benefits, however, such solutions require that a third party intermediary provide and verify information about all participating individuals and organizations. In addition, concerns abound that the third party that operates the centralized repository will become a significant target that governments and criminals will desire access to in order to track agents' Web communications and, subsequently, invade their privacy to a substantial degree. For instance, the U.S. Government has requested various technology companies to provide back-door access to their hardware for investigative purposes (Dickson, 2015), and many criminal attacks have gained illegal access to third party systems and stolen personal information (Basu, 2015). As of yet, we do not know about any research that has investigated the willingness of individuals to use a system that promises to protect their online security at the cost of their privacy.

Research that examines users' perceptions related to privacy in online environments is certainly not new. In fact, information systems (IS) researchers have engaged in information privacy research for many years (Bélanger & Crossler, 2011). Privacy calculus represents one aspect of information privacy that has been particularly informative of individuals' engagement in online transactions (e.g., e-commerce) (Dinev et al., 2006). Privacy calculus posits that individuals perform a cognitive assessment between costs and benefits to determine whether they will enter into transactions online (Smith, Dinev, & Xu, 2011). These factors include weighing the perceived benefits of yielding personal information with the perceived risks of doing so. In general, if the benefits of releasing personal information outweigh the risks of doing so, then an individual will be more likely to enter into a transaction. This foundational privacy research, however, does not consider one's benefit being a secure environment (i.e., ecosystem) to conduct future and probably sensitive transactions with other agents. Such an environment provides its own set of paradoxical privacy concerns and other concerns that hackers or third parties such as governments present (as we discuss above).

In addition to privacy calculus, the more broad foundation of social exchange theory (SET) (Blau, 1964; Cropanzano & Mitchell, 2005) can help one to understand the cost-benefit tradeoff, which users who use any network infrastructure to exchange sensitive data will likely experience. Specifically, costs beyond loss of privacy are important considerations for individuals before they engage in activities with other individuals and organizations. In any case, the costs and benefits involved in such tradeoffs involve both intangible and economic-based factors (Gefen & Ridings, 2002).

What is unique about our research relative to previously examined contexts, however, is that the relationship between information security and privacy protection appear to be at odds with one another in the proposed ecosystem. Individuals generally undertake information security efforts as a means to protect private information, but trusted identity ecosystems require individuals to give up their private information to a third party intermediary so it can verify all users who transmit data. By having a third party intermediary monitor users' activities and require them to verify themselves, these systems promise to increase users' information security. Few would doubt that the Internet is an open environment that allows anyone to use it and engage in transactions (March, Hevner, & Ram, 2000). Of course, this same freedom allows uninvited parties to enter the transaction stream and capture information thought to be secure (Callegati, Cerroni, & Ramilli, 2009). However, we remain to see whether individuals will knowingly relinquish information privacy for the sake of improved security.

The foundations of privacy calculus and its predecessor, SET, suggest that a wide variety of costs and benefits are likely associated with individuals' decisions to use an infrastructure that offers benefits at the request of a complete loss of privacy—albeit to a supposed independent and unbiased third party. The issue that remains unanswered, then, is whether and why individuals would be willing to completely sacrifice their privacy to one entity for the tradeoff of a secure computing environment. As we note above, this context is unique and still in its infant stages; thus, we adopted a mixed-methods approach whereby findings derived from focus groups rather than previous literature informed our conceptual model. By using two methodologies, questions could emerge from the target population that may not have emerged from the literature alone (Venkatesh et al., 2013). In particular, we interviewed focus groups to understand how they would respond to a system such as the identity ecosystem. We then used the concepts expressed during the focus group as we reviewed existing

support from the extant literature to build an emergent conceptual model. We then assessed this model quantitatively using data obtained from a cross-sectional survey via SEM to determine which of the elicited factors drive individuals' willingness to use the proposed environment.

3 Methodology

Because the E.U. and the U.S. Governments' proposed identity ecosystems do not yet exist in mature form, we have much to discover about users' perceptions of the future system. When existing research models or strong findings do not exist, IS researchers have embraced critical qualitative approaches as viable and adequate alternatives to study Information Technology (IT) problems (Orlikowski & Baroudi, 1991; Richardson & Robinson, 2007; Stahl & Brooke, 2008; Trauth & Jessup, 2000). One such critical qualitative approach that has gained visibility and popularity in ill-defined, under-researched, or relatively new IS fields is the focus group (Miles & Huberman, 1994; Sobreperez, 2008). Focus groups allow the participants on the research topic to interact with and respond to the questions and issues presented by the moderator(s) and other participants on a specific topic (Krueger & Casey, 2000). The approach allows researchers to go in-depth into the topic of interest by understanding the circumstances of their participants' opinions (Bélanger, 2012).

Researchers have used focus groups to examine a variety of IS topics, such as the alignment of business and IS (Campbell, Kay, & Avison, 2005), mobile technology use (Choi, Lee, Im, & Kim, 2007; Jarvenpaa & Lang, 2005), IT delivery options (Geissler, Zinkhan, & Watson, 2001; Smith & McKeen, 2007), post-installation use of enterprise resource planning (Jones, Zmud, & Clark, 2008), and collaboration in IT (Smith & McKeen, 2011). Indeed, the number of studies and the quality of journals that publish research based on this method illustrate the increasing importance and acceptance of focus groups as an appropriate research method in IS (Bélanger, 2012). The use of standard data-collection techniques such as interviews or non-participatory observations might not allow the researcher to understand the extent to which participants similarly perceive constructs. Accordingly, focus groups offer valuable insight into IS phenomena by embedding individuals into collectives (Morgeson & Hofmann, 1999), which, in turn, affects their perceptions and reactions. The interaction among the individuals in the focus groups helps to form conceptual IS models, which is core to the IS field's growth (Bélanger, 2012).

Using focus groups for the theory-development purpose (Bélanger, 2012) of understanding the under-researched issue of the privacy-security tradeoff can be extremely useful. Thus, we began this exploratory phase of research to identify possible explanations as to why individuals would sacrifice their privacy to increase security during their activities online. We conducted a total of five focus group sessions, and each session comprised two to twelve undergraduate and graduate students with an overall total of 34 participants. Previous literature states that one needs to select members of the focus group based on the knowledge about the topic investigated (Bélanger, 2012). Thus, we selected undergraduate and graduate IS students in the US as our participants given that they represent the "Internet" generation whose members tend to be aware of privacy and security in the online environment (American Press Institute, 2015; Zorabedian, 2015). Furthermore, given that the NSTIC proposed the identity ecosystem that we used as the reference to generate discussion, selecting respondents in the US was appropriate.

We conducted all the focus group studies in a private room at the university to which the students attended. Each focus group session lasted approximately 30 to 45 minutes. We designed the interview guide with open-ended questions to not limit participants' potential responses, which is especially important in exploratory research such as ours (Cohen & Crabtree, 2006; Turner, 2010). We designed the sessions to accommodate the different participants who had varying levels (i.e., beginner to advanced) of understanding regarding online privacy and security. Each researcher moderated at least one focus group using the same interview guide and following the same protocol. In first few minutes of the focus groups, we focused on educating participants about our study's objectives to help them understand that there was no right or wrong answers to any of the questions and to build rapport with them. The moderator led the participants in a discussion with general items, such as how they used their time when using the Internet (e.g., websites visited, data entered, types of searches). After this initial conversation, we asked more detailed questions regarding members' password hygiene, computer security practices, concern for information privacy, and any previous privacy-breach experiences. Finally, we briefly described the proposed identity ecosystem (i.e., the NSTIC) to the respondents (see Appendix A). We gave participants two minutes to review the description, after which they could ask clarification questions if needed. Afterwards, we discussed whether they would use such a system and the justification for their opinions. While the moderators used the same interview guide to be able to make valid comparisons with the data

collected from the focus group sessions, the semi-structured nature of the sessions allowed the moderators to ask impromptu questions to extract further information that they might not have expected while following the interview guide (Cohen & Crabtree, 2006; Wengraf, 2001).

The moderators were aware of the fact that participants needed to be involved at a high level to ensure they all voice their opinions about the topic and that they needed to probe further whenever appropriate (Sobreperez, 2008). Thus, the moderators made the utmost effort to make the environment as informal and communicative as possible. We captured the dialogues during the focus groups via tape recordings with permission from the participants and the authors reviewed them after the focus group sessions finished. Once we transcribed these recordings, we worked independently to analyze the content in order to place the qualitative data into nodes (Braun & Clarke, 2006). Following the assignment of content to the various nodes, we discussed the few discrepancies that existed in how we named the nodes until we agreed on the naming conventions. In addition, no new nodes emerged as we analyzed the focus group session transcriptions, which signaled that we had reached a saturation point with our data collection and that we did not need to conduct any further focus groups (Glaser & Strauss, 1967; Guest, Bunce, & Johnson, 2006). Figure 1 presents the conceptual model that emerged from this exercise. In Section 4, we present the findings from the focus groups and the resulting conceptual model and then discuss our quantitative assessments of the emergent model.

4 Analysis

Prior to analyzing the data, we transcribed the focus group recordings. We independently analyzed the resulting transcriptions, which resulted in the emergence of several key response themes. We compared the resulting themes and standardized the naming conventions. Where discrepancies existed between the coding efforts—which were few—we discussed their reasoning and reached agreement. A research model emerged from this analysis. The model comprised three broad categories that influence an individual's intentions to use an identity ecosystem such as the one mentioned by the NSTIC: 1) intrapersonal characteristics, 2) perceptions of the controlling agent, and 3) perceived system characteristics. In Sections 4.1 to 4.4, we present the components of each of these factors that comprise our overall theoretical model and present example quotes from focus group participants.

4.1 Intrapersonal Characteristics

The intrapersonal factors refer to characteristics about potential users of the system that would either prohibit or promote their adopting and using an identity ecosystem. These factors comprise the following components: 1) censorship attitude, 2) self-efficacy, 3) behavioral-based inertia, and 4) previous similar experience.

4.1.1 Censorship Attitude

One significant barrier to adoption that the participants raised was their attitude toward possible censorship of their activities. Similar to the attitude toward Internet censorship (Wang & Mark, 2015), we refer to the more general attitude toward censorship as people's attitude towards someone in a position of power's limiting their expression. Since the government and other third party organizations will be heavily involved in developing, operating, and monitoring identity ecosystems, respondents showed considerable concern that they could censor any activities taking place therein as one respondent stated[1]:

> *And if it's government, it will be much easier for them to control information and the Web. My only concern will be if the US government finds some information to be offensive and deem it unnecessary for American people to read or whatever. It will be that much easier for them to cut off our access then. I am not saying that they would do that, but there's always some kind of thought in the back of my mind.*

As the respondent's statement illustrates, she indicated concern that the government would be able to make a determination as to whether information was offensive and, if so, cut off access to that information. This possibility is an example of her attitude towards government censoring data that causes concern for using an identity ecosystem. Given comments of this nature, the likelihood that people will use an identity ecosystem will be lower if they believe that their information will be censored.

[1] Appendix B provides additional quotes that support these components.

4.1.2 Self-efficacy

In response to follow-up questions about how they address the security issues they identified when using the Internet, respondents indicated that they used several methods to handle Internet-based security threats on their own. Thus, some respondents believed they had the capability to protect themselves without the need for an identity ecosystem. For example, one respondent stated:

> *It depends, if I am using something important like a PayPal account, then I will use some long and complicated password…but if it's like my YouTube account in which I have no money or nothing important, then I put something easy to remember.*

We have assigned this and similar responses to the topic of self-efficacy, which we define as "the belief that one has the capability to perform a particular behavior" (Compeau & Higgins, 1995, p. 189). As the respondent's statement illustrates, he felt that he had the ability, or self-efficacy, to use different passwords of varying strengths to provide adequate protection on different websites. Therefore, given his belief that he could engage in protective action on his own, the likelihood that he would use an identity ecosystem in the future would be lower than one exhibiting lower levels of self-efficacy.

4.1.3 Behavioral-based Inertia

Some respondents stated that using the system needed to be a consistent activity that they performed. Either they would become accustomed to using it for all of their tasks or they would not use it for any of their tasks. Respondents indicated that they might already be using a system that provided similar services and would likely continue doing so because that was what they were used to doing. In other words, the current way of operating on the Internet seems appropriate simply because that is what they have always done. These individuals seemed to indicate that habits were important to them, and performing the same behavior consistently drove their behavior. We draw on Polites and Karahanna (2012) and refer to this factor as behavioral-based inertia, which implies "that the use of a system continues simply because it is what the individual user has always done, and therefore without giving it much, if any, thought" (p. 24) as one respondent indicated:

> *I mean you can't please everybody at the same time not requiring them to join the network…..so just tell them that if you don't want to come to the castle then stay outside on the equal playing field.*

As this respondent's statement illustrates, he felt that people's use of a system is an all-or-nothing decision that they should not customize to please all of someone's desires. This thought suggests that what people are used to doing drives their behavior, which fits the definition of behavioral-based inertia. As such, we expect that the stronger entrenched someone's behavioral-based inertia, the less likely they will be to use an identity ecosystem.

4.1.4 Similar Previous Experience

Finally, when asked whether they had experienced a system similar to the one described, a few respondents noted that it was similar to one that they had used in the military. The respondents who had experience with this system indicated that they believed that it worked effectively. They also indicated that, if the proposed system were like the military system, they would use it. For example, one respondent stated:

> *The military system. Their CAC [Common Access Card] card holds our information and when you go to the military base, that's what you use to log in to their base.*

Based on the experience that these respondents expressed, we expect that the more experience a user has with a system similar to an identity ecosystem, the more likely they are to use the identity ecosystem.

4.2 Perceptions of the Controlling Agent

The second major theme of the comments provided through the focus groups, perceptions of the controlling agent, refer to an individual's assessment of how they view the party who is responsible for providing this system. These perceptions comprised trustworthiness, reputation, and privacy concerns.

4.2.1 Trustworthiness and Reputation

Individuals expressed multifaceted decisions for why they would give up privacy completely to gain security via the identity ecosystem that the NSTIC suggests. On one hand, future users want to protect their privacy in online transactions as security attacks become more sophisticated: on the other, these same individuals worry whether censorship of the activities they now enjoy will be too great a hurdle to overcome for protection against that sophistication. In addition, individuals' intentions to use the proposed ecosystem appear to be largely based on three factors of trustworthiness that previous researchers have identified in organizational settings: 1) ability, 2) benevolence, and 3) integrity (Mayer, Davis, & Schoorman, 1995). Note that the NSTIC initiative calls on collaborative efforts between public and private entities; thus, some of the comments received refer to private organizations that respondents mentioned in the focus groups as parties they would like to see join forces with the U.S. Government. One illustrative comment regarding the need for trustworthiness in such a system follows:

> *I mean if you are paying for service like that, you are paying them to protect your identity and stuff like that. That's their job. I would trust them if they have not had anything go wrong in the past few years and they are using that money to help me facilitate the need to protect my personal information, I can trust with that party. No problem.*

As this respondent's statement illustrates, she found trust to be an important factor to consider prior to entering into a relationship with an organization to protect her information. When an organization has a history of demonstrating that they do not violate their customers' trust in general, then that history increases the likelihood that people will trust them with their information. As such, we expect that the more people trust an organization, the more likely they will use that organization's identity ecosystem.

Of the participants' major concerns, trust and reputation of those involved with the development and operations of the proposed infrastructure dominated the discussions. For example, one respondent stated:

> *And it's all about reputation…. The reputation of "hey, that's what we are here for and we do a good job and you can trust us". I wouldn't automatically jump to somebody like that unless I hear what they were to say about what that they were going to do….. Their reputation matters.*

As this respondent mentioned, the reputation that a company has determines whether or not he trusts them. If a company has a poor reputation, then he will not trust them. Given this comment, we expect that a company's reputation will have a positive relationship on how much they are trusted.

4.2.2 Privacy Concerns

Respondents also expressed concerns about their privacy online. While we expected that privacy concern would emerge from the focus groups, the detail about those concerns was telling. Respondents suggested that, although they had concerns about their privacy, they were still somewhat naïve to the privacy ramifications of their Internet behaviors. One factor where there was a disconnect between respondents' privacy concerns and their privacy behaviors related to the control of information. For example, one respondent said:

> *That does seem to be an issue. I know somewhere someone is keeping record of what I am doing at all times…. People are keeping record of that for whatever purposes. That's still kind of weird. I feel like I am not myself anymore…. Somebody else is being me as well.*

Others indicated the privacy related to protecting information about where they lived and were not as concerned about information related to what they did on the Internet. An illustrative example of one such comment is: "I don't put anything on the Internet that I don't want other people to know about. That's the only concern I have that I don't want to give information about where I live or stuff like that.".

These two previous comments are interesting in that they highlight two divergent actions taken due to privacy attitudes toward using the Internet. In the former comment, the respondent indicated that people were keeping track of her and her actions at all times but yet continued using the Internet as usual despite noting that it was "weird" to her. In the latter comment, the respondent was aware of privacy implications to his information and modified his Internet behavior accordingly.

Other participants acknowledged the concerns for their privacy but indicated that the benefits they received from social networking offset the potential harm they received from going against their privacy concerns. For example, one respondent stated:

> *I don't know. I think that's the risk we take when we go online. We don't have to give information online or the Internet but that's the risk we take to live socially online.*

However, some participants indicated that they tried to take control of the information that they put on social networks so that they could control their privacy. This finding suggests that different behaviors do exist depending on the level of a person's privacy concerns as one respondent expressed:

> *With privacy, as long as you don't post anything too personal about where you live or what not, then I think you will be somewhat ok. I pretty much keep my Facebook account clean because even if you have these privacy settings or only some friends can see these things, and someone logs into your account then he can see what's in there. And I forgot to log off at one computer at a different area at one of my family members' homes and that ended up causing a headache to my account and I thought it was by hacker until I was able to track it down. So, as far as privacy, I try to restrict as much information I put onto the web that I am comfortable with.*

These previous two comments indicate that Internet users engage in a privacy calculus (Dinev et al., 2006) where they weigh the benefits of sharing information with the privacy concerns or cost of sharing that information. In the former example, the respondent indicated that the social benefits of enjoying the Internet were worth the costs of giving up his information. In the latter example, the respondent indicated that her concern for privacy was not worth the benefit of giving up that information—especially after a negative experience on social media. Thus, given these various concerns related to privacy and the potential impact it has on behaviors, we expect that privacy concerns, in general, will influence people's use of an identity ecosystem, although this influence could have substantial variation across individuals.

4.3 Perceived System Characteristics

The third and final major component of the model that emerged from the focus groups, perceived system characteristics, refers to issues related to the system itself and how it would function. We refer to these factors as system granularity, response efficacy, and perceived inconvenience.

4.3.1 System Granularity

When asked if they would use a system such as the identity ecosystem, respondents indicated that it would depend on whether they could use the system for various Web activities as they saw fit as opposed to being limited to a few specialized activities. One respondent stated this belief as follows:

> *For day to day use like browsing the Internet or looking up news or anything where I don't put in any information, this system isn't necessary. It's only necessary for something where I am transacting over the Internet that requires personal identifying information that I am most concerned with.*

In this example, the respondent did not believe that she needed the identity ecosystem for consuming information on the Internet via browsing sessions. She did, however, like the idea of having the granular control of being able to use the identity ecosystem when entering into transactions online.

However, some respondents indicated that they did not think the system would be useful unless a person were completely committed to using it. For example, one respondent said:

> *I mean I am on for giving people choices and stuff, but for something like this, it doesn't make sense. Because the whole point is to protect you, and the system is there to make sure that people can't steal your identity. If you're going to join the system and not even use it, what's the purpose of it?*

Accordingly, this respondent indicated that he did not believe that having the ability to choose when to use the identity ecosystem would provide the level of protection that people desired from the identity ecosystem.

These differing views on how users could selectively alter when and how they use an identity ecosystem suggest that the ability to control what one uses the identity ecosystem for is an important consideration. Therefore, we refer to this factor as system granularity and expect that the level of granularity that an identity ecosystem provides will influence a person's intention to use it.

4.3.2 System Efficacy

During the focus groups, several respondents mentioned previous security breaches that affected them personally. For example, one respondent said:

> *For example, I did a transaction on the Internet. I think some kind of fraud happened because all of a sudden I had $2,000 worth of transactions on my credit card. I didn't know what specific actions I did. Luckily for me, my bank was able to resolve it. It's a huge issue to see that something of so big an amount on your credit card statement.*

Another respondent similarly stated:

> *That happened to me. My credit card was stolen. They wiped out my whole bank account. I had to go to the bank and resolve it. It was a big deal.*

In both of these comments, individuals evidently expected and relied on the systems they used to effectively thwart attacks and enable them to take corrective action should something go amiss. Given this backdrop, any proposed identity ecosystem would need to actually protect its users rather than merely state that it would do so. Thus, system efficacy, or a proposed system's ability to effectively limit information security threats, is an important consideration for potential adopters of the new system.

4.3.3 Perceived Inconvenience

As a final system characteristic, focus group participants discussed the potential drawback of personal inconvenience to use the proposed identity ecosystem. For example, one respondent said:

> *The other thing that will concern me is that participation could be day-to-day or transaction-to-transaction choice. That could be very inconvenient for users to have to go through this specific system before they could even do anything.*

This respondent's comment indicates that making choices about whether to use an identity ecosystem on a regular basis would cause an inconvenience. Unfortunately, inconvenience would likely lead to lack of system use. As such, we believe that perceptions of inconveniences will reduce the likelihood that one will use an identity ecosystem.

4.4 Contextual Factors

Finally, it emerged from the focus group participants that they would use a system such as the identity ecosystem for their Internet activities given various different contextual factors. Prior information systems research also suggests that context specification is an important aspect of understanding the phenomena one studies (Hong, Chan, Thong, Chasalow, & Dhillon, 2014). As such, we explore the factors that emerged from our focus groups, which include Web activity, Web location, and network type.

4.4.1 Web Activity

Participants mentioned that, while useful, they would not need the new network for all types of activity on the Web. For example, one recipient said:

> *I don't need that for everything, maybe except for when my social security and credit card numbers are needed. As far as I am concerned, I would pay for it…but I don't need it for everything.*

Thus, this respondent indicated that needed the protections of the identity ecosystem only for transferring sensitive information such as social security numbers and credit card numbers. This and other comments suggest that individuals would more likely use an identity ecosystem when dealing with specific Web activity rather than general Web activity.

4.4.2 Web Location

In addition, participants perceived where they would access the Internet (e.g., at home, in the office, public facility) to be an important factor in choosing to use the new infrastructure. One respondent said: "Depends on where I am at. I mean, I am not going to buy stuff through credit card if I am on library with Internet. But if I am in my home, I feel more secured.".

This respondent's comment shows that her being in a public location away from home, such as the library, increased her need for changing her Web usage behavior. Thus, we expect that people will be more inclined to use an identity ecosystem when they are in open, public locations than when they are at a more secure location, such as their home.

4.4.3 Network Type

Finally, future users would likely assess the type of Internet connection (i.e., wired or wireless) available when forming intentions to use the proposed identity ecosystem. As one respondent said:

> *When I began using wireless networks, I was not as concerned as now and would jump at the network to use the Internet or check my email...not knowing the security holes that were involved or people can jump on those open network. Now, I make sure that I am only in open network if I have things to do that aren't important so that I don't have important information stolen.*

Similar to physical location of the network, this respondent indicated that the type of network he was using drove the Web behavior he would engage in. Specifically, when on wireless networks, he did not conduct sensitive tasks to avoid having his information stolen. As such, we expect that the type of network used will influence identity ecosystem usage such that users will more likely use an identity ecosystem when they are on a wireless network.

Figure 1 presents the emergent research model. In Section 5, we discuss how we assessed this emergent model empirically.

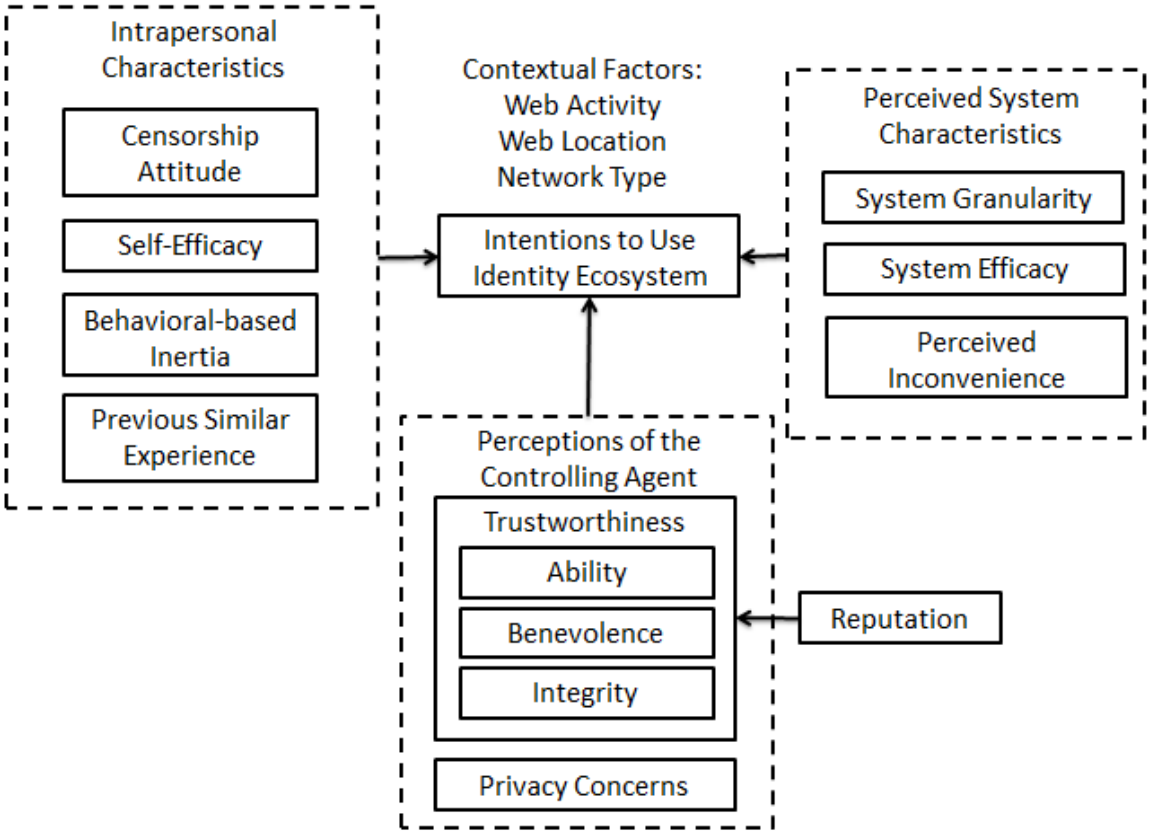


Figure 1. Emergent Research Model

5 Test of Nomological Net

To address the lack of statistical validity inherent with using focus groups (Nielsen, 1997), we empirically analyzed our research model. We adapted previously validated measures for our survey and then pilot tested the resulting instruments to ensure their validity. Following this initial assessment, we conducted a

full-scale survey with a sample of respondents (n = 362) from Amazon's Mechanical Turk that represented the adult Internet population in the US.

5.1 Pilot Test

In order to initially assess our adaptations of the previously published construct measures, we issued the survey to students enrolled in an MBA program at a large public institution in the Southern United states (n = 69). The students were in their second semester of their four-semester program. Forty-four percent of the students were male. They had an average age of 24.74 years (SD = 2.70 years) with a minimum and maximum age that ranged from 22 to 33 years, respectively. Eighty percent stated that they had used a personal computer for general reasons for more than a decade, and 64 percent reported using the Internet for more than a decade. Additionally, over half of the pilot sample (i.e., 50.7%) reported to have known about an online security breach that affected them personally.

We used the data we obtained from the pilot sample (including qualitative comments about the survey items) to evaluate the validity of our adapted survey instruments. Following the traditional assessments of internal consistency and convergent and discriminant validities, we deemed the items to be appropriate adaptations to the identity ecosystem context.

5.2 Data Collection

For our main data-collection efforts, we issued the survey on Amazon's Mechanical Turk. Mechanical Turk is an online crowdsourcing market that researchers can use to find individuals to participate in studies. Respondents are paid and participate in cognitive tasks, such as taking online surveys and participating in online experiments (Brandon, Long, Loraas, Mueller-Phillips, & Vansant, 2014; Steelman, Hammer, & Limayem, 2014). In all, 411 participants who lived in the United States and were at least 18 years of age responded. As with the focus groups, participants needed to fulfill the former criterion because our context was the identity ecosystem that the NSTIC and President Obama proposed. We dropped seven responses for failing the attention check question during the first set of questions and 42 responses for failing a second attention check question to indicate whether they understood a description of the proposed NSTIC program. As such, we conducted the final analysis with data from 362 respondents.

Respondents' average age was 35.01 years (SD = 10.94) with a minimum and maximum age that ranged from 19 years to 65 years, respectively. The 53.6 percent male sample were fairly well educated: 90.2 percent had some college or more, and 53.5 percent had at least a bachelor's degree. Eighty-eight percent reported having more than a decade experience using a computer for general reasons, and 84.0 percent reported using the Internet for more than 10 years. Nearly 75 percent responded that they had never been personally affected by an online security breach.

Unless stated otherwise, we collected all items on a seven-point Likert scale that ranged from "strongly disagree" to "strongly agree". For ease of reference, we referred to the trusted identity ecosystem indicated by the NSTIC as the "Government Internet" in the survey and associated construct instruments. Appendix C presents the items we used in collecting data and their sources, loadings, AVEs, composite reliabilities, and Cronbach's alphas. We briefly discuss them below. After removing a few items, all constructs demonstrated acceptable discriminate and convergent validity and reliability.

5.3 Intrapersonal Characteristics

We assessed general censorship attitude with the instrument from Hense and Wright (1992) and retained four of its five items. We assessed self-efficacy with the instrument from Workman et al. (2008) and retained three of its five items. We assessed behavioral-based inertia with the three-item measure for behavior-based inertia from Polites and Karahanna (2012) and retained all items. We used three items to measure similar experience (Jarvenpaa, Tractinsky, & Vitale, 2000) and retained all items.

5.4 Perceptions of the Controlling Agent

As previous research and our focus group results suggest, trustworthiness comprises three facets: ability, benevolence, and integrity (Mayer & Davis, 1999; McKnight, Choudhury, & Kacmar, 2002). The ability measure contained four items. We assessed benevolence via a five-item instrument. Finally, we used a four-item measure to assess integrity. Together, these three components reflected the second-order construct that constituted trustworthiness. We used the four-item organization reputation scale from

Turban, Forret, and Hendrickson (1998) to assess the government reputation. We assessed privacy concern via the four-item Internet privacy concern scale (Dinev & Hart, 2006a). We retained all items that reflected constructs in the perceptions of the controlling agent portion of our model.

5.5 Perceived System Characteristics

We assessed system granularity with a four-item measure of perceived behavioral control (Ajzen & Madden, 1986; Madden, Ellen, & Ajzen, 1992) and retained all items. We measured system efficacy and perceived inconvenience via adaptations from previous work (Workman, Bommer, & Straub, 2008). We retained three items from five for system efficacy and all three items for perceived inconvenience.

5.6 Behavioral Intention

Finally, the focus groups identified various conditions in which they would possibly use a Government Internet, which included 1) using the Internet in general versus to share highly sensitive information such as online banking details, 2) using a public versus private Internet connection, and 3) surfing the Internet wirelessly versus over a wired connection. Therefore, we adapted six different three-item behavioral-intention constructs from previous research (Pavlou, 2003), which included general Web activity, banking Web activity, home Internet access, public Internet access, wired network connection, and wireless network connection.

5.7 Controls

In addition to the constructs in our emergent model, we collected demographic data to use as potential controls in our quantitative assessments. We captured information about respondents' age, gender, education, income level, years of experience in general computing, and years of experience in using the Internet. As we note above, we also asked whether the respondents had previously been personally affected by an online information privacy/security breach.

6 Data Analysis

Given that we focus on determining the factors that best predict individuals' intentions to use a system that offers increased security at the expense of information privacy, we chose to rely on component- rather than covariance-based structural equation modeling (SEM). In particular, we chose to use SmartPLS 3.0 (Ringle, Wende, & Becker, 2014) for all of our analyses. By using SEM, we could determine the relative importance of each of the factors that the focus groups identified in explaining variance in individuals' intentions to use the system and assess both measurement and structural models simultaneously.

We assessed the validity of our constructs' instruments by examining convergent and discriminant validities. For convergent validity, all of our instruments exhibited Cronbach alphas and composite reliabilities well above the common 0.70 threshold. Further, most items loaded at 0.70 or above on their respective constructs, and the average variance extracted (AVEs) values were greater than 0.50. Thus, we concluded that our instruments exhibited strong convergent validity.

For the purposes of discriminant validity, we assessed the cross loadings of the individual items. All of the items loaded at least 0.10 higher on their respective constructs than other constructs in the conceptual model (Gefen & Straub, 2005). Further, all zero-order correlations (see Appendix D) were less than the square root of the AVEs of each construct involved in the correlation (Fornell & Larcker, 1981). Therefore, the measurement instruments displayed adequate discriminant validity, and the assessment of the structural paths was appropriate.

In addition to the validity assessments, we also determined the possible degree that common methods variance (CMV) could affect our data and subsequent analyses. For this purpose, we conducted the Harman's one-factor test (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003), which indicated that CMV was not present to a significant degree. Specifically, Harmon's one-factor test revealed the first of the factors that emerged from an unrotated principal components assessment explained only 37.2 percent of the total variance among all items, and a rotated Varimax solution indicated that the factor that exhibited the largest eigenvalue explained 13.2 percent of the items' variance. Thus, a single factor was not responsible for explaining a majority of the items' variance. Therefore, we feel comfortable that the presence of CMV was not strong enough so as to negatively affect our assessments and findings.

Before assessing the conceptual model for each context (i.e., Web activity, location, and network type), however, we evaluated the degree to which only the control variables explained variance in intentions. The controls of age, years of experience in general computing, and years of experience in using the Internet were not significant; thus, we removed them from further examination. The other four control variables of gender, income, education, and having been previously compromised due to an online security breach remained in the assessment of the entire conceptual model for each context. Table 1 displays the results of the analysis of the control variables and the entire conceptual model.

Table 1. Findings from PLS-SEM Analysis

	Web activity		Web location		Network type	
Behavioral intention	General	Banking	Home	Public	Wired	Wireless
Controls[†]						
Compromise	0.091	0.085	0.076	0.057	0.059	0.057
Education	0.095	0.100	0.080	0.100*	0.075	0.119*
Gender	0.163**	0.130*	0.147**	0.150**	0.160**	0.164***
Income	0.095*	0.069	0.096	0.111*	0.130**	0.089
Intrapersonal characteristics						
H1. Censorship attitude	0.155**	0.049	0.132***	0.106*	0.124**	0.079
H2. Self-efficacy	-0.022	-0.107**	-0.052	-0.079	-0.065	-0.068
H3. Behavioral-based inertia	-0.130*	-0.095*	-0.175***	-0.083	-0.126**	-0.136**
H4. Previous similar experience	0.139**	0.023	0.110**	0.067	0.116*	0.127***
Perceptions of the controlling agent						
H5. Trustworthiness	0.162*	0.288***	0.191**	0.186*	0.255***	0.245***
H6. Privacy concerns	-0.097	-0.104	-0.100	-0.025	-0.099	-0.059
Perceived system characteristics						
H7. System granularity	-0.028	0.006	-0.033	0.042	-0.023	-0.001
H8. System efficacy	0.169**	0.120	0.161*	0.251***	-0.065	0.151*
H9. Perceived inconvenience	-0.143*	-0.204***	-0.195**	-0.157*	-0.182**	-0.220***
R^2	0.485	0.515	0.568	0.478	0.520	0.580

[†]The results for the controls are from the controls-only model, whereas all other results are from the complete model with controls included; results are standardized beta coefficients (p-values); * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

7 Discussion

7.1 Implications for Research

Findings emerging from our mixed-methods approach identified several key groups of factors relevant to individuals' decisions to use identity ecosystems despite the inherent privacy issues. Specifically, we identified three general categories of constructs that influence these intentions: 1) intrapersonal characteristics of the adopter, 2) perceived characteristics of the controlling agent, and 3) perceived system characteristics. Thus, while the general privacy calculus and social exchange literatures help explain privacy-related behaviors by weighing costs and benefits associated with an action, we expand on this framework in our context to include these three distinct categories. Had we simply relied on the privacy calculus or social exchange foundations for our research, we would have very likely never identified the constructs that emerged from our focus groups to include in our conceptual model, which indicates that one's decision to use an identity ecosystem goes beyond the factors typically implemented in privacy calculus research.

Of the intrapersonal characteristics, censorship attitude (H1), behavioral-based inertia (H3), and previous experience with systems similar to the proposed identity ecosystem (H4) were significant across most of the usage contexts. Interestingly, however, the directionality of the relationship between censorship attitude and usage intentions was opposite of what we expected. Specifically, those who had general

concerns regarding censorship were *more likely* to use the identity ecosystem than those who were not. We contribute this finding to two possible reasons. First, many U.S. citizens believe that they have the right to speak freely (i.e., freedom of speech) and that the U.S. Government should uphold this right. In other words, those individuals who focus on this right believe and expect the government will protect it whether in the physical or digital world. An identity ecosystem overseen to some degree by the U.S. Government should defend individuals' speech in that environment. Second, when it comes to comments and discussion on the Internet in general, it is not unusual for comments to be completely turned off or for a loud vocal group of individuals to shout down and silence any voices that might want to participate in the conversation (BBC, 2015). In this instance, individuals who believe that censorship should not be allowed would view an identity ecosystem as a place where this type of behavior would not occur.

Another interesting finding relates to self-efficacy (H2). In several security-related studies, self-efficacy is one of the most strongly supported relationships (e.g., Crossler, Long, Loraas, & Trinkle, 2014; Johnston & Warkentin, 2010; Lee & Larsen, 2009). However, in our study, self-efficacy was significant only in the banking context and in a negative direction. This finding might be due to the contextual nature of this environment versus the Web in general, which is in line with how Marakas, Johnson, and Clay (2007) suggest that IS studies should use self-efficacy. Because information security studies use self-efficacy in both the general (e.g., Anderson & Agarwal, 2010; Herath & Rao, 2009; Ifinedo, 2012) and context-specific natures (Herath et al., 2014; Johnston & Warkentin, 2010; Lee & Larsen, 2009), researchers should rely on context specificity when investigating the tradeoff between privacy and security protections. On the other hand, individuals who believe they have the capability to protect themselves without using an additional mechanism might be less likely to use an identity ecosystem in a banking context over others simply because of the level of sensitivity that exists with online financial transactions.

Of perceptions of the controlling agent, trustworthiness (H5) (as expressed as a second-order construct that reflects ability, benevolence, and integrity) was highly significant in explaining variance in intentions to use the identity ecosystem (average $\beta = 0.221$) across all possible usage contexts. This finding is extremely important in that future users of identity ecosystems evaluate the controlling agent's capability to offer a secure environment (i.e., ability), desire to "do good" (i.e., benevolence), and honesty (i.e., integrity). In an environment with potential privacy issues that stem from identity-verification processes that use sources other than user-supplied information and future monitoring and surveillance activities, trustworthiness factors are paramount in individuals' adoption decisions. Conversely, if potential users do not see the provider as trustworthy, then they do not see whatever protections they offer as worth the tradeoff. In fact, despite a sizable zero-order correlation of -0.531 between privacy concerns (H6) and intentions, privacy concerns were not significant in explaining intentions in any of the six contexts, which indicates that trustworthiness is much more important than general privacy concerns in an identity ecosystem environment.

Of perceived system characteristics, system efficacy (H8) and perceived inconvenience (H9) were significant in four and all six of the contexts, respectively. Thus, future adopters of identity ecosystems expect a system that effectively minimizes security threats from unknown sources but does not become inconvenient.

A few of the constructs that emerged from the focus groups as possible antecedents to intentions to use the Government Internet exhibited insignificant relationships in the empirical assessment when we considered all factors simultaneously. Specifically, system granularity (H7) failed to explain significant variation in behavioral intentions regardless of Web activity, location, or network type. Our reasoning for this lack of significance is that respondents fully believed that the identity ecosystem would be a choice-based solution. In other words, respondents understood that users of the future identity ecosystem could choose when they would route their Internet traffic through the controlled infrastructure and when they would simply use the existing public Internet infrastructure. We believe that, had respondents been presented with a solution that did not allow such a choice, H7 would have been significant.

Surprisingly, however, general privacy concerns (H6) also lacked significant influence on our dependent variable in all cases, though its relationship with behavioral intentions approached significance in some instances. This finding could be due to the fact that respondents understood that all traffic in the identity ecosystem would be monitored and that users of the system—whether individuals or organizations—

would first need to provide necessary information about their identities prior to gaining access to the controlled environment. In summary, our data confirms seven of our nine hypotheses.[2]

These findings also provide an initial look into factors that would lead to people's adopting and using a solution that addresses potential solutions resulting from the Bright ICT Initiative (Lee, 2015). In particular, we provide details regarding the basic conditions that normal citizens view as important in adopting a system such as the one that the NSTIC has proposed. For example, individuals are generally concerned about adopting identity ecosystems if they must break previous routines they have become accustomed to (i.e., behavioral-based inertia), if they believe that they can protect themselves from security threats while using the public Internet infrastructure (i.e., self-efficacy), and the costs of inconvenience are greater than any perceived benefits from using the identity ecosystem. Conversely, individuals who have experienced similar systems (e.g., military ID card systems); who believe that the controlling agents associated with the identity ecosystem are trustworthy in terms of benevolence, integrity, and ability; and who perceive that the system will actually live up to its proposed benefits (i.e., system efficacy) are likely to adopt the identity ecosystem for at least some of their online activities. Of all these constructs elicited from the focus groups, trustworthiness and inconvenience appeared to be the most consistently significant factors across all of the contexts.

From a theoretical standpoint, our research validates the assertion that individuals make multifaceted decisions when deciding whether to use a future identity ecosystem. Individuals account for factors that have a positive and negative bearing on their intentions to use the new system. Additionally, these factors do not solely concern the agent responsible for controlling and monitoring access and activity on the ecosystem or the system characteristics themselves; rather, research must also consider intrapersonal characteristics. Had we not engaged in a mixed-methods approach and, thus, not used focus groups, we would have likely failed to uncover the factors of censorship attitude, behavioral-based inertia, and system granularity. Therefore, at least in the context of identity ecosystems, an initial reliance on privacy calculus would have been detrimental since, in particular, general privacy concerns failed to exert any significant influence on intentions to use the identity ecosystem across the various contexts.

7.2 Implications for Practice

From a practical standpoint, developers and moderators of any future identity ecosystem must provide information to potential users that includes their ability to deal with information security threats effectively. In addition to ability, future users must also perceive that the controlling agent(s) have the users' best interests at heart (i.e., benevolence) and that they will handle the information they collect with care (i.e., integrity). These factors combine to form perceptions of trustworthiness, which is a necessary condition for individuals to use an identity ecosystem. Developers must also work to alleviate users' concerns about perceived inconveniences about using the new system. Given that the systems such as the ones that the NSTIC specify are granular in nature, our findings suggest that potential users will not use them if the perceived inconvenience in using the system overall and in a piecemeal (i.e., activity by activity) fashion become too large a hurdle.

Further, our findings suggest that identity ecosystems' developers and marketers should not use individuals' general privacy concerns as a promotion mechanism. Given that privacy concern's association (i.e., correlation) with intentions was fairly strong in our study, some might be tempted to focus on that element to drive adoption. However, privacy concern's influence on adoption was significantly minimized across all contexts when we considered other factors simultaneously.

Finally, our findings suggest that people who would use identity ecosystems would do so because they desire increased protection of their ability to act and speak freely online. Practitioners should keep this issue in mind as they build and develop an environment that protects individuals' speech while ensuring a safe online environment.

8 Limitations and Future Research

As with any research study, our research has limitations. First, we presented the identity ecosystem to our participants as a hypothetical, but real, situation that had not yet been instituted. In doing so, we could explore individuals' intentions to adopt such a system because none were currently using one. As pilot

[2] The relationship between reputation and trustworthiness was highly significant (i.e., $\beta = 0.700^{***}$, t-score = 24.197; $R^2 = 0.490$); however, because the relationship did not have a direct bearing on respondents' intentions to adopt the identity ecosystem, we chose to remove it from the table that displays the other relationships in the conceptual model.

identity ecosystems come online (Kreft, 2014), researchers will have an opportunity to test individuals' actual adoption behavior rather than their intentions only in the near future. Research that focuses on those individuals who have the opportunity to participate in a pilot study would shed further light on this phenomenon, especially after the individuals have used the system for some trial period. It will be particularly interesting to see whether users perceive the benefits that the major ecosystem proposals and their use cases describe, such as securing smart phone transactions, securing business operations, and enhancing public safety (NIST, 2015), as benefits that continue to outweigh the tradeoff in personal privacy.

Second, we used college students for the focus groups. This approach may have limited some of the issues that the participants raised in that other, different types of participants may have raised other issues. However, we somewhat controlled for this possible limitation by validating the model with respondents from Amazon Mechanical Turk. The demographics of this group better represented the population of the US as a whole.

From a design science perspective, this study provides an insightful look at what it would take for identity ecosystems to attract potential adopters. Future research could build on these findings to guide the development of a system with these findings as part of the kernel theory that drives the research (Kuechler & Vaishnavi, 2012). This approach would be especially important as part of the Bright ICT Initiative as the AIS works with the United Nations to create safe Internet solutions for the existing Internet environment.

Future research could also explore design facets in an identity ecosystem in order to limit personal efforts involved in accessing and using the identity ecosystem. One could execute such research as a practical research effort to increase participation rates due to the large influence perceived inconvenience had on intention to use the ecosystem. For example, one could create trusted identities and determine whether inconvenience could be attributed to becoming a trusted identity before actual use occurs. In other words, future research should assess whether inconvenience more strongly relates to gaining authorized access to (i.e., one-time cost) or actually using an identity ecosystem (i.e., recurring cost).

Finally, it is interesting to note that, though a control variable, gender was a surprisingly strong factor that influenced intentions. However, when we tested the complete model, this influence vanished. The fact that men expressed higher self-efficacy towards using such a system than women could explain why. This finding is not surprising since previous research has also found that men express a higher level of computer self-efficacy (Crossler & Bélanger, 2009). On the other hand, we expected previous compromises to have a more significant influence as a control than they did, and future research should explore why they did not.

9 Conclusions

In this study, we provide an initial investigation into the reasons why individuals would be willing to surrender personal privacy to a third party intermediary for the sake of security while using the Internet via recently proposed identity ecosystems. Because of the unique context inherent in such a system, we diverged from relying on previous privacy-calculation foundations and explored the issue afresh with a mixed-methods approach. Three important categories of factors relating to individuals' intentions to use identity ecosystems in the future emerged from our focus groups: 1) intrapersonal characteristics of the adopter, 2) perceived characteristics of the controlling agent, and 3) perceived system characteristics. We then assessed this model via structural equation modeling and ascertained that the perceived trustworthiness (i.e., benevolence, integrity, and ability) of the agent who creates and maintains the ecosystem—the government in our specific case here—is paramount. Individuals also rely on their perceptions of system efficacy and perceived inconvenience to drive their intentions. Unexpectedly, we found that censorship attitude plays a role in potential use decisions such that those who are more sensitive about censorship activities are more likely to use the system that those who are less sensitive.

In summary, the factors that emerged from our analyzing focus group interviews explained at least 47 percent of the variance in intentions to use identity ecosystems across six different use contexts. Our findings highlight the importance that trustworthiness plays in evaluating tradeoffs in identity ecosystems; thus, other studies that explore solutions to address the AIS Bright ICT Initiative moving forward should include it. Furthermore, by exploring the use of an identity ecosystem from many different levels of granularity, we demonstrate that researchers need to pay attention to the conditions in which their theory is supported. As the theory is tested in different contexts, it may not generalize to all situations. We encourage future researchers to expand on our work by incorporating existing theories with these findings

to help shed light on the mental calculations individuals experience when considering cost-benefit tradeoffs such as the one that identity ecosystems demand.

Acknowledgments

We thank the Southeastern Conference (SEC) for providing funding that partially supported this research.

References

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Englewood Cliffs, NJ: Prentice-Hall.

Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology, 22*(5), 453-474.

American Press Institute. (2015). *Digital lives of millennials*. Retrieved, from http://www.americanpressinstitute.org/publications/reports/survey-research/digital-lives-of-millennials/

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

Barrett, D. (2016). Apple-FBI phone fight gets technical. *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/apple-fbi-phone-fight-gets-technical-1456101154

Basu, E. (2015). Cybersecurity lessons learned from the Ashley Madison hack. *Forbes.* Retrieved from http://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/

BBC. (2015). *Is it the beginning of the end for online comments?* Retrieved from http://www.bbc.com/news/blogs-trending-33963436

Bélanger, F. (2012). Theorizing in information systems research using focus groups. *Australasian Journal of Information Systems, 17*(2), 109-135.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041.

Bélanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3), 245-270.

Blau, P. M. (1964). *Exchange and power in social life.* New York, NY: J. Wiley.

Brandon, D. M., Long, J. H., Loraas, T., Mueller-Phillips, J., & Vansant, B. (2014). Online instrument delivery and participant recruitment services: Emerging opportunities for behavioral accounting research. *Behavioral Research in Accounting, 26*(1), 1-23.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Bria, F., Ruiz, J., Clavell, G. G., Zavala, J. M., Fitchner, L., & Halpin, H. (2015). *D3.3 research on identity ecosystem: D-CENT.* Retrieved from https://dcentproject.eu/wp-content/uploads/2015/10/research_on_digital_identity_ecosystems.pdf

Buckovich, S. A., Rippen, H. E., & Rozen, M. J. (1999). Driving toward guiding principles a goal for privacy, confidentiality, and security of health information. *Journal of the American Medical Informatics Association, 6*(2), 122-133.

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-middle attack to the https protocol. *IEEE Security & Privacy, 7*(1), 78-81.

Campbell, B., Kay, R., & Avison, D. (2005). Strategic alignment: A practitioner's perspective. *Journal of Enterprise Information Management, 18*(6), 653-664.

Choi, H., Lee, M., Im, K. S., & Kim, J. (2007). Contribution to quality of life: A new outcome variable for mobile data service. *Journal of the Association for Information Systems, 8*(12), 598-618.

Cohen, D., & Crabtree, B. (2006). *Qualitative research guidelines project.* Retrieved from http://www.qualres.org/HomeSemi-3629.html

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-212.

Cropanzano, R., & Mitchell, M. S. (2005). Social exchange theory: An interdisciplinary review. *Journal of Management, 31*(6), 874-900.

Crossler, R. E., & Bélanger, F. (2009). The effects of security education training and awareness programs and individual characteristics on end user security tool usage. *Journal of Information System Security, 5*(3), 3-22.

Crossler, R. E., Long, J., Loraas, T., & Trinkle, B. (2014). Understanding compliance with BYOD (bring your own device) policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209-226.

d-cent. (2013). *Research on identity ecosystem.* Retrieved from http://dcentproject.eu/wp-content/uploads/2015/10/research_on_digital_identity_ecosystems.pdf

Dickson, B. (2015). How much privacy is too much? *TechCrunch.* Retrieved from http://techcrunch.com/2015/11/24/how-much-privacy-is-too-much/

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce—a study of Italy and the United States. *European Journal of Information Systems, 15*(4), 389-402.

Dinev, T., & Hart, P. (2006a). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80,100.

Dinev, T., & Hart, P. (2006b). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

Dyck, J. J., & Pearson-Merkowitz, S. (2013). The privacy generation. *Pacific Standard.* Retrieved from http://www.psmag.com/navigation/politics-and-law/privacy-generation-security-spying-nsa-government-67394/

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Gefen, D., & Ridings, C. M. (2002). Implementation team responsiveness and user evaluation of customer relationship management: A quasi-experimental design study of social exchange theory. *Journal of Management Information Systems, 19*(1), 47-70.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*, 91-109.

Geissler, G., Zinkhan, G., & Watson, R. T. (2001). Web home page complexity and communication effectiveness. *Journal of the Association for Information Systems, 2*(1), 1-46.

Gibbs, M. (2011). NSTIC and the feds HUA problem. *NetworkWorld.* Retrieved from http://www.networkworld.com/article/2198827/security/nstic-and-the-feds-hua-problem.html

Glaser, B., & Strauss, A. (1967). *The discovery of grounded theory: Strategies of qualitative research*. London, UK: Wiedenfeld and Nicholson.

Goss, P. (2013). A little less privacy is worth a little more security, says internet founder. *TechRadar.* Retrieved from http://www.techradar.com/us/news/world-of-tech/a-little-less-privacy-is-worth-a-little-more-security-says-internet-founder-1178398

Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L. (2014). *History of information: The case of privacy and security in social media.* Paper presented at the Proceedings of the History of Information Conference.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods, 18*(1), 59-82.

Hense, R., & Wright, C. (1992). The development of the attitudes toward censorship questionnaire. *Journal of Applied Social Psychology, 22*(21), 1666-1675.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*(1), 61-84.

Herath, T., & Rao, H. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research, 25*(1), 111-136.

Howard, P. N. (2014). Data breaches in Europe: Reported breaches of compromised personal records in europe, 2005-2014. *Center for Media, Data and Society*. Retrieved from http://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope.pdf

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *National Institute of Standards and Technology*. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Jarvenpaa, S. L., & Lang, K. R. (2005). Managing the paradoxes of mobile technology. *Information Systems Management, 22*(4), 7-23.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management, 1*(1-2), 45.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 548-566.

Jones, M. C., Zmud, R. W., & Clark, T. D., Jr. (2008). ERP in practice: A snapshot of post-installation perception and behaviors. *Communications of the Association for Information Systems, 23*, 437-462.

Kreft, E. (2014). Government to test “identity ecosystem” in two states: Sound scary? It is. *TheBlaze*. Retrieved from http://www.theblaze.com/stories/2014/05/06/government-to-test-identity-ecosystem-in-two-states-sound-scary-it-is/

Krueger, R. A., & Casey, M. (2000). *A practical guide for applied research*. London: Sage.

Kuechler, W., & Vaishnavi, V. (2012). A framework for theory development in design science research: Multiple perspectives. *Journal of the Association for Information Systems, 13*(6), 395-423.

Lee, J. K. (2015). Guest editorial: Research framework for AIS grand vision of the bright ICT initiative. *MIS Quarterly, 39*(2), iii-xii.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executive's decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin, 18*(1), 3-9.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (Iuipc): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Marakas, G. M., Johnson, R. D., & Clay, P. F. (2007). The evolving nature of the computer self-efficacy construct: An empirical investigation of measurement construction, validity, reliability and stability over time. *Journal of the Association for Information Systems, 8*(1), 16-46.

March, S., Hevner, A., & Ram, S. (2000). Research commentary: An agenda for information technology research in heterogeneous and distributed environments. *Information Systems Research, 11*(4), 327-341.

Mayer, R. C., & Davis, J. H. (1999). The effect of the performance appraisal system on trust for management: A field quasi-experiment. *Journal of Applied Psychology, 84*(1), 123-136.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334-359.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook.* Thousand Oaks, CA: Sage.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs, 35*(1), 27-44.

Morgeson, F. P., & Hofmann, D. A. (1999). The structure and function of collective constructs: Implications for multilevel research and theory development. *Academy of Management Review, 24*(2), 249-265.

Nielsen, J. (1997). The use and misuse of focus groups. *IEEE Software, 14*(1), 94-95.

NIST. (2015). *The identity ecosystem: Use examples*. Retrieved from http://www.nist.gov/nstic/identity-ecosystem.html

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1-28.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101-134.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & 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), 879-903.

Polites, G. L., & Karahanna, E. (2012). Shackled to the status quo: The inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. *MIS Quarterly, 36*(1), 21-42.

Pritchett, B. (2015). AIS bright Internet ties with UN ITU. *Association for Information Systems*. Retrieved from https://aisnet.org/news/266591/-AIS-Bright-Internet-Ties-with-UN-ITU.htm

Richardson, H., & Robinson, B. (2007). The mysterious case of the missing paradigm: A review of critical information systems research 1991-2001. *Information Systems Journal, 17*(3), 251-270.

Ringle, C. M., Wende, S., & Becker, J. (2014). *SmartPLS 3*. Retrieved from http://www.smartpls.de

Rojas, H., Shah, D. V., & Faber, R. J. (1996). For the good of others: Censorship and the third-person effect. *International Journal of Public Opinion Research, 8*(2), 163-186.

Schneier, B. (2008). What our top spy doesn't get: Security and privacy aren't opposites. Retrieved from http://archive.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0124

Smith, H. A., & McKeen, J. D. (2007). Developments in practice xxvii: Delivery IT functions: A decision framework. *Communications of the Association for Information Systems, 19*, 725-739.

Smith, H. A., & McKeen, J. D. (2011). Enabling collaboration with IT. *Communications of the Association for Information Systems, 28,* 243-254.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1015.

Sobreperez, P. (2008). Using plenary focus groups in information systems research: More than a collection of interviews. *Electronic Journal of Business Research Methods, 6*(2), 181-188.

Stahl, B. C., & Brooke, C. (2008). The contribution of critical IS research. *Communications of the ACM, 51*(3), 51-55.

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly, 38*(2), 355-378.

Sternstein, A. (2011). Former CUA director: Build a new Internet to improve cybersecurity. *Nextgov.* Retrieved from http://www.nextgov.com/nextgov/ng_20110706_1137.php

Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting patient privacy and data security. *New England Journal of Medicine, 368*(11), 977-979.

Tomhave, B. (2011). Identity crisis: The delusion of NSTIC. *The Falcon's View.* Retrieved from http://www.secureconsulting.net/2011/04/identity-crisis-the-delusion-o.html

Trauth, E. M., & Jessup, L. M. (2000). Understanding computer-mediated discussions: Positivist and interpretive analyses of group support system use. *MIS Quarterly, 24*(1), 43-80.

Turban, D. B., Forret, M. L., & Hendrickson, C. L. (1998). Applicant attraction to firms: Influences of organization reputation, job and organizational attributes, and recruiter behaviors. *Journal of Vocational Behavior, 52*(1), 24-44.

Turner, D. W., III. (2010). Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report, 15*(3), 754-760.

Venkatesh, V., Brown, S., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly, 37*(1), 21-54.

Wang, D., & Mark, G. (2015). Internet censorship in china: Examining user awareness and attitudes. *ACM Transactions on Computer-Human Interaction, 22*(6), 31:31-31:22.

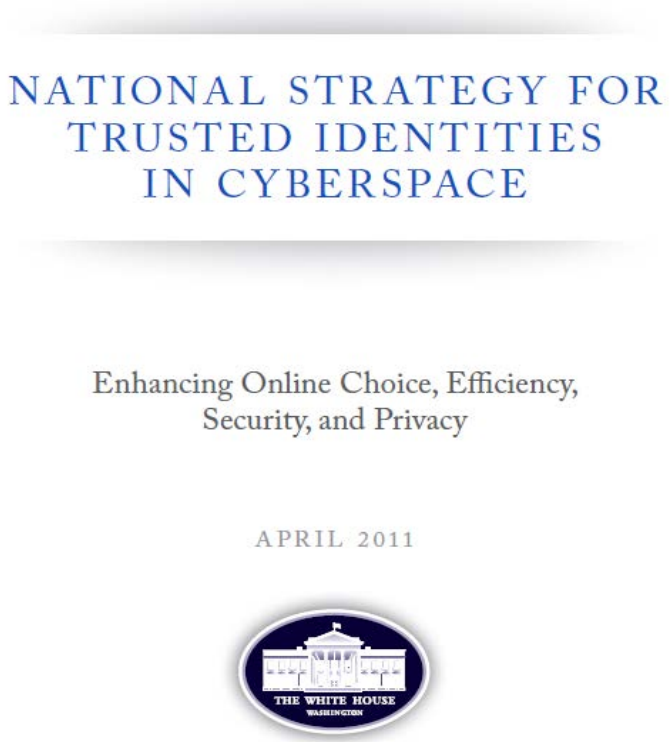
Wengraf, T. (2001). *Qualitative research interviewing: Biographic narrative and semi-structured methods.* London, UK: Sage.

Whitehead, J. W. (2011). Identity ecosystem: Big brother logs on. *The Rutherford Institute*. Retrieved from https://www.rutherford.org/publications_resources/john_whiteheads_commentary/identity_ecosystem_big_brother_logs_on

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Zorabedian, J. (2015). It's time we stopped calling millennials "dumb" about data privacy. *Naked Security.* Retrieved from https://nakedsecurity.sophos.com/2015/07/08/its-time-we-stopped-calling-millennials-dumb-about-data-privacy/

Appendix A



In April 2011, U.S. President Barack Obama issued *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy* (NSTIC). This initiative is in response to the need for individuals and companies to conduct activities over the Internet without the potential security threats to such activities. The Internet is not owned or controlled by any one individual, company, or nation. This makes ensuring that its users are not affected by security threats such as identity theft and online fraud a difficult task.

To help alleviate these security issues, the NSTIC recommends that public and private institutions collaborate to create an *Identity Ecosystem. An Identity Ecosystem* would be a private network based on the public Internet wherein all participants, their computer systems, and their activities are authenticated via credentials. These credentials are attributes about an individual or computer system provided by pieces of hardware like smart cards or third party providers similar to PayPal's business model with eBay transactions. These credentials would provide important information about the participants (e.g., age, gender, employment status); however, the overall goal of the private network would be to verify the characteristics of the user without providing the user's actual identity to other users. Additionally, the *Identity Ecosystem* would be built according to the following guiding principles:

1. Identity solutions will be privacy-enhancing and voluntary
2. Identity solutions will be secure and resilient (i.e., ability to recover from potential difficulties)
3. Identity solutions will be interoperable (i.e., ability to work with one another)
4. Identity solutions will be cost-effective and easy to use

Regarding individuals' choice in using the new private network, the following is a direct quote from NSTIC:

> *Participation in the Identity Ecosystem will be voluntary: the government will neither mandate that individuals obtain an Identity Ecosystem credential nor that companies require Identity Ecosystem credentials from consumers as the only means to interact with them Individuals shall be free to use an Identity Ecosystem credential of their choice, provided the credential meets the minimum risk requirements of the relying party, or to use any non-Identity Ecosystem mechanism provided by the relying party Individuals' participation in the Identity Ecosystem will be a day-to-day—or even a transaction-to-transaction—choice.*

Appendix B

Table B1. Focus Group Components with Quotes

Components	Additional example quotes
Censorship attitude	*I mean you won't have freedom for certain things, you know.*
Self-efficacy	*I use this image thing…. You have your image that you have chosen for years and see it every time…. If it's not there, I don't log in or use that website.*
Behavioral-based inertia	*I just don't see why you would want to choose transaction by transaction……I want to opt into more secure network but then I will do it in an insecure way.*
Similar previous experience	*It's the military "super nuper" net. They were just like that.*
Trustworthiness and reputation	*Maybe Microsoft. I think people trust them now because with Xbox they have online payment and you pay monthly service to them. Nothing has happened… so far. I trust Microsoft.* *You trust it and then something goes wrong. What would you do about it? That trusted network no longer becomes trusted.* *I have to trust the company. That's what it comes down to. How much do you trust them?* *The Government is definitely the one place that tries to have the highest possible security because they have to protect our nation. Now still, there's little bit of concern as you hear about guy who takes the laptop and with all the information, he releases to public. So, there's always that concern but government has lot higher standard than others companies would do.*
Privacy concerns	*I am not too concerned about what I do as I believe that I know enough about what's out there, I am more concerned about how others handle my information. I know how to reset privacy settings in Facebook or to browse the Internet safely. Now if the company has their data compromised, then that's more of the security concern I am worried about… especially about financial information.* *See, that's what creeps me out. For example, I might go to iTunes and buy a book and they might send me email about other books from the author. That's ok, but they are keeping information with them that I didn't give them. They are taking it anyways.*
System granularity	*If they allow me to choose which transactions, I would feel comfortable making purchases through it.*
System efficacy	*The Government is definitely the one place that tries to have the highest possible security because they have to protect our nation. Now still, there's little bit of concern as you hear about guy who takes the laptop and with all the information, he releases to public. So, there's always that concern but government has lot higher standard than others companies would do.* *If Government takes control, then there could be the possibility that it could be safe. This means that you are in a more controlled environment…. To me it is like that.* *It's an analogy of having a locker or a safety deposit in a bank. That's more like a locker in internet place and your identity is safe over there. So that's the best thing and I think that's needed over here because in locker there is all kind of identity stored over there. If you want to access, you will need to go to that place to have access. And it should have all different kind of security measures involved over there.*
Web activity	*For day to day use like browsing Internet or looking up news or anything where I don't put up any information, this system isn't necessary. It's only necessary for something where I am transacting over the Internet that requires personal identifying information that I talked about earlier that I am most concerned with.*
Web location	*Like, when I am on an open network, somewhere in a coffee shop or Starbucks, I try not to go anywhere or do anything like online shopping.*
Network type	*Sometimes you can use the VPN. I use the campus VPN for certain things. So I am using their Internet through another Internet. That way it's more secured.* *That's what I do when I use credit card to pay my bills or shop. I usually do it only if I am connected to an Ethernet line.*

Appendix C

Table C1. Survey Items

Construct items	Mean (σ)	CR	α
System granularity (adapted from Ajzen & Fishbein, 1980; Madden et al., 1992) If I wanted to I could easily choose if and when to use the Government Internet. I would have complete control of choosing if and when I used the Government Internet.	3.37 (0.991)	0.956	0.939
Censorship attitude (adapted from Rojas, Shah, & Faber, 1996) All individuals should have the right to openly express their ideas, no matter how prejudiced they might be. Everybody should have full liberty of propagandizing for what they believe to be true. Demonstrations/rallies by controversial political groups should be restricted (reverse coded).	1.62 (0.693)	0.910	0.870
Behavioral-based inertia (adapted from Polites & Karahanna, 2012) I will continue using my existing method for accessing the Internet simply because it is what I have always done. I will continue using my existing method for accessing the Internet simply because it is part of my normal routine. I will continue using my existing method for accessing the Internet simply because I've done so regularly in the past.	3.68 (0.913)	0.971	0.956
Similar experience (adapted from Jarvenpaa et al., 2000) I frequently use a system similar to the Government Internet. I regularly use a system similar to the Government Internet. I often connect to the Internet using a system similar to the Government Internet.	1.97 (0.878)	0.978	0.967
Government ability (adapted from Mayer & Davis, 1999) The government is capable of providing Internet security and privacy. The government has much knowledge about maintaining users' Internet security and privacy. The government is qualified to handle Internet security and privacy matters.	2.63 (0.960)	0.937	0.910
Government benevolence (adapted from McKnight et al., 2002; Mayer & Davis (1999)) I feel that the government would act in the Internet user's best interest when it comes to Internet privacy and security. My needs and desires towards Internet privacy and security are very important to the government. The government would not knowingly do anything to hurt my Internet privacy and security.	2.40 (1.007)	0.936	0.915
Government integrity (adapted from McKnight et al., 2002; Mayer & Davis, 1999) I will never have to wonder whether the government will stick to its word regarding Internet privacy and security. I am comfortable relying on the government to meet their obligations regarding Internet privacy and security. I feel fine with the proposed Internet security as well as privacy since the government generally fulfills its agreements.	2.11 (0.898)	0.932	0.903
Government reputation (adapted from Turban et al., 1998) The government has a reputation of being an excellent watchdog for people's information privacy and security. When it comes to people's information privacy and security, the government has a good public image. I have heard a lot of good things about the government in regard to maintaining people's information privacy and security. The government has an excellent reputation among people in maintaining people's information privacy and security.	1.85 (0.823)	0.952	0.933

Table C1. Survey Items

Privacy concerns (adapted from Dinev & Hart, 2006b) I am concerned that a third party can find private information about me in Government Internet. I am concerned about submitting information on the Government Internet because of what others might do with it. I am concerned about submitting information on the Government Internet because it could be used in a way I did not foresee.	4.10 (0.799)	0.948	0.926
System efficacy (adapted from Workman et al., 2008) The available measures which can be taken by the government to protect my personal information from Internet security threats would be effective. The preventive measures available to the government to stop Internet threats from harming my personal information would be adequate.	2.69 (0.992)	0.966	0.948
Self-efficacy (adapted from Workman et al., 2008) For me, taking information security precautions to protect my personal information from Internet threats is easy. I have the necessary skills to protect my personal information from information security threats on the Internet. My skills required to stop Internet security threats against my personal information from being successful are adequate.	3.31 (0.891)	0.925	0.878
Inconvenience (adapted from Workman et al., 2008) Using the newly proposed Government Internet would be so much of a nuisance that I think that I would be better without it. The negative side effects of using the Government Internet would be greater than the advantages.	3.37 (1.081)	0.921	0.872
Behavioral intentions—general Web activity (adapted from Pavlou, 2003) I intend to use the Government Internet for general web surfing activities. I expect to utilize the Government Internet for general web surfing activities. It is likely that I will transact through the Government Internet for general web surfing activities.	2.02 (0.928)	0.974	0.960
Behavioral intentions—banking Web activity (adapted from Pavlou, 2003) I intend to use the Government Internet for my online banking activities. I expect to utilize the Government Internet for my online banking activities. It is likely that I will transact through the Government Internet for my online banking activities.	2.27 (1.128)	0.988	0.981
Behavioral intentions—home Internet access (adapted from Pavlou, 2003) I intend to use the Government Internet when using the Internet at home. I expect to utilize the Government Internet when using the Internet at home. It is likely that I will transact through the Government Internet when using the Internet at home.	2.09 (0.965)	0.979	0.967
Behavioral intentions—public Internet access (adapted from Pavlou, 2003) I intend to use the Government Internet when using the Internet in a public location. I expect to utilize the Government Internet when using the Internet in a public location. It is likely that I will transact through the Government Internet when using the Internet in a public location.	2.46 (1.142)	0.976	0.964
Behavioral intentions—wired network connection (adapted from Pavlou, 2003) I intend to use the Government Internet when using the Internet plugged directly into the wall. I expect to utilize the Government Internet when using the Internet plugged directly into the wall. It is likely that I will transact through the Government Internet when using the Internet plugged directly into the wall.	2.05 (0.907)	0.970	0.953
Behavioral intentions—wireless network connection (adapted from Pavlou, 2003) I intend to use the Government Internet when using the Internet wirelessly. I expect to utilize the Government Internet when using the Internet wirelessly. It is likely that I will transact through the Government Internet when using the Internet wirelessly.	2.18 (0.993)	0.979	0.968

Appendix D

Table D1. Inter-construct Correlations

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1. Ability	**0.888**																	
2. Benevolence	0.677	**0.864**																
3. Censorship	0.255	0.284	**0.846**															
4. Compromise	0.054	0.064	-0.033	**NA**														
5. Education	0.098	0.016	-0.005	0.003	**NA**													
6. Gender	0.118	0.160	0.171	-0.061	-0.084	**NA**												
7. Granularity	0.273	0.318	-0.005	0.070	0.021	0.092	**0.919**											
8. Income	0.078	0.110	0.004	0.008	0.274	-0.001	0.092	**NA**										
9. Inconvenience	-0.596	-0.591	-0.100	-0.051	-0.012	-0.164	-0.272	-0.076	**0.892**									
10. Inertia	-0.225	-0.262	-0.110	-0.019	-0.060	-0.081	0.014	-0.022	0.463	**0.958**								
11. Integrity	0.757	0.833	0.310	0.043	-0.009	0.151	0.311	0.041	-0.612	**-0.260**	**0.880**							
12. Previous experience	0.216	0.317	0.183	0.044	0.011	0.051	0.154	0.107	-0.248	-0.199	0.297	**0.968**						
13. Priv. concern	-0.503	-0.598	-0.241	-0.071	0.070	-0.070	-0.213	0.038	0.605	0.356	-0.655	-0.350	**0.905**					
14. Reputation	0.573	0.653	0.370	0.031	-0.052	0.154	0.213	-0.021	-0.403	-0.163	0.690	0.247	-0.556	**0.913**				
15. Self-efficacy	-0.038	-0.002	-0.149	0.114	-0.119	-0.180	0.041	0.077	0.133	0.187	-0.043	0.034	0.040	0.037	**0.897**			
16. System efficacy	0.741	0.689	0.197	0.061	0.060	0.102	0.359	0.105	-0.645	-0.242	0.715	0.279	-0.532	0.506	-0.090	**0.951**		
17. Trustworthiness	0.873	0.927	0.310	0.059	0.035	0.158	0.330	0.085	-0.654	-0.273	0.944	0.306	-0.642	0.700	-0.028	0.778	**0.802**	
18. Intentions	0.556	0.581	0.233	0.075	0.104	0.108	0.224	0.088	-0.604	-0.367	0.616	0.261	-0.531	0.419	-0.179	0.588	0.638	**0.982**

Bolded lines on the diagonal represent the square of the average variance extracted (AVE).

About the Authors

Robert E. Crossler is an Assistant Professor in the Carson College of Business at Washington State University. His research focuses on behavioral information security and privacy decisions of individuals. Crossler's award winning information privacy and security research has been published in top journals in Information Systems such as *MIS Quarterly*, *Information Systems Journal*, *Decision Support Systems,* and *Computers & Security*. His research in information privacy has been recognized by the INFORMS Information Systems Society with their 2013 Design Science Award. His research in information security was recognized by *The DATA BASE for Advances in Information Systems* as the paper of the year in 2014. He currently serves as the Treasurer for the Security Special Interest Group (SIGSEC) of the Association for Information Systems and is an active member of the IFIP Working Group 8.11/11.13 Information Systems Security Research.

Clay Posey is an Associate Professor of Management with a joint appointment in the Institute for Simulation & Training at University of Central Florida. His main research interests focus on information security and privacy with a particular emphasis on behavioral information security within organizations. He has received extramural financial support for these efforts from the U.S. Department of Defense Personnel Security Research Center in Monterey, CA, and the IBM Center for the Business of Government. He has presented his research at various national and international conferences and has published work in outlets such as *MIS Quarterly, Journal of Management Information Systems, European Journal of Information Systems, Information & Management,* and *Computer & Security,* among others. He currently serves as an Associate Editor at *Information & Management* and is an active member of the IFIP Working Group 8.11/11.13 Information Systems Security Research.