Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Understanding Consumers' Attitudes Toward Controversial Information Technologies: A Contextualization Approach

Michael Breward, Khaled Hassanein, Milena Head

To cite this article:
Michael Breward, Khaled Hassanein, Milena Head (2017) Understanding Consumers' Attitudes Toward Controversial Information Technologies: A Contextualization Approach. Information Systems Research

Published online in Articles in Advance 24 Jul 2017

. https://doi.org/10.1287/isre.2017.0706

http://pubsonline.informs.org/journal/isre/

INFORMATION SYSTEMS RESEARCH
Articles in Advance, pp. 1–15
ISSN 1047-7047 (print), ISSN 1526-5536 (online)

Understanding Consumers' Attitudes Toward Controversial Information Technologies: A Contextualization Approach

Michael Breward,[a] **Khaled Hassanein,**[b] **Milena Head**[b]

[a] Faculty of Business and Administration, University of Winnipeg, Winnipeg, Manitoba R3B 2E9, Canada; [b] DeGroote School of Business, McMaster University, Hamilton, Ontario L8S 4M4, Canada

Contact: m.breward@uwinnipeg.ca (MB); hassank@mcmaster.ca (KH); headm@mcmaster.ca, http://orcid.org/0000-0002-4329-3654 (MH)

Received: July 26, 2010
Revised: December 15, 2011; July 31, 2013; April 6, 2015; December 7, 2016
Accepted: December 22, 2016
Published Online in Articles in Advance: July 24, 2017

https://doi.org/10.1287/isre.2017.0706

Abstract. Controversial information technologies, such as biometrics and radio frequency identification, are perceived as having the potential to both benefit and undermine the well-being of the user. Given the type and/or amount of information these technologies have the capability to capture, there have been some concerns among users and potential users. However, prominent technology adoption models tend to focus on only the positive utilities associated with technology use. This research leverages net valence theories, which incorporate both positive and negative utilities, and context of use literature to propose a general framework that can be used for understanding consumer acceptance of controversial information technologies. The framework also highlights the importance of incorporating contextual factors that reflect the nuances of the controversial technologies and their specific context of use. We apply the framework to consumer acceptance of biometric identity authentication for banking transactions through automated teller machines. To that end, we contextualize the core construct of perceived benefits and concerns to this domain in a qualitative study of 402 participants, determine the appropriate contextual factors that are antecedents of the contextualized core constructs by examining relevant past research, and then develop and validate a contextualized research model in a quantitative study of 437 participants. Findings support the validity of our framework, with the model explaining 77.6% of the variance in consumers' attitudes toward using biometrics for identity authentication at automated teller machines.

History: Vishwanath Venkatesh, Senior Editor and Associate Editor.
Funding: This project was funded by a grant from the Ontario Research and Development Challenge Fund.
Supplemental Material: The online appendix is available at https://doi.org/10.1287/isre.2017.0706.

Keywords: controversial information technology • user acceptance of IT • contextualization • biometric identity authentication

1. Introduction

Information technology (IT) acceptance has been at the forefront of information systems research for over three decades (Venkatesh et al. 2016). Given the ever increasing pace of both the development of new ITs and the degree to which individuals and organizations alike rely on these new technologies to accomplish their daily personal and work tasks, it is imperative that we continue to examine what drives IT acceptance. This is especially true for emerging ITs for which there is a threatening or controversial side due to the natural concerns they elicit with potential users, which hinders their widespread acceptance. We define a controversial IT as one that is generally perceived as having the potential to both benefit and undermine the well-being of the user. Generally speaking, concerns related to controversial ITs tend to be focused on privacy and/or security (Chen and Zhao 2012, Hossain 2014, Patil and Seshadri 2014, Patil et al. 2015, Tene and Polonetsky 2012). Thus, ITs that have endemic privacy and security concerns are typically considered controversial. Examples of such controversial ITs include biometrics and radio frequency identification (RFID). Given the type and/or amount of information these technologies have the capability to capture, concerns among users and potential users exist. However, prominent technology adoption models tend to focus on the expected positive utility of using a particular technology while ignoring possible concerns that can affect consumers' attitudes. A net valence approach that considers both benefits and concerns will be valuable when studying the adoption of controversial technologies where people are predisposed to view such technologies with skepticism. The context in which controversial ITs are deployed can also affect consumer attitudes (Hossain and Dwivedi 2014). Thus, we must rethink and appropriately contextualize existing IT adoption models, which were initially developed for noncontroversial technologies, before using them to understand user acceptance of such controversial ITs.

Such contextualization can lead to rich theoretical and practical insights (Johns 2006, Hong et al. 2014).

Studying the adoption of controversial ITs continues to be underexplored in the literature (Baker et al. 2010, Miltgen et al. 2013), and without identifying the factors that promote or impede acceptance of such technologies, user acceptance will continue to trail the pace of development. This reality is unfortunate, as these controversial ITs have the potential to significantly and positively influence individuals, organizations, and society by reducing identity fraud (biometrics), cutting costs throughout the supply chain (RFID), more effectively identifying and addressing customer needs (big data), and giving smaller businesses and consumers access to more computing power (cloud computing). We seek to address this gap by understanding what drives consumers' attitudes toward using controversial ITs, taking into account their perceived benefits and concerns from a net valence perspective. Specifically, we examine biometric technologies as an example of controversial ITs because their potential for identity authentication has been identified both by the public and private sectors.

We therefore aim to (i) develop a general research framework to understand controversial IT acceptance based on net valence decision-making theories and context of use literature and (ii) demonstrate the utility of this framework by developing a contextualized research model to understand consumer adoption of a specific controversial IT (biometric identity authentication for accessing bank accounts at automated teller machines (ATMs).

2. Theoretical Background

Peter and Tarpey (1975) refer to a cognitive-rational consumer decision-making model in which consumers behave in a rational manner, where they are goal directed, calculated, and predicated on some knowledge of the benefits and costs of various alternatives available. They associate this model with three possible decision-making approaches: (i) a *perceived risk* approach in which consumers try to minimize any negative utility, (ii) a *perceived return* approach in which consumers try to maximize expected utility, and (iii) a *net valence* approach in which consumers try to maximize net returns or net valence by assessing the difference between the expected positive and negative utilities. Historically, technology adoption models have employed a net return perspective, focusing on the expected positive utility of technology adoption (Cazier et al. 2008). Notwithstanding the importance of perceived benefits of an IT in shaping consumers' attitudes and/or intentions toward that technology, when examining consumer acceptance of controversial ITs, the influences of perceived negative aspects, such as fear, cannot be overlooked (Kulviwat et al. 2007, Mick and Fournier 1998). Given people's predisposition to view the unknown with skepticism and worry, it stands to reason that the more controversial the IT, the greater the need to consider the impact of concerns on technology adoption. Cazier et al. (2008) stress the significant and innovative contribution of examining both positive and negative utility for technology acceptance, especially in the realm of controversial ITs.

Culnan and Armstrong (1999) utilized a net valence reasoning in the context of consumer privacy where they note that consumers engage in a decision process they refer to as a *privacy calculus*. Culnan and Bies (2003) liken an individual's privacy calculus to an internalized cost–benefit analysis in which the individual discloses personal information if the resulting benefits equal and hopefully surpass their assessment of the risk of disclosure. This privacy calculus has been further expanded by others (e.g., Dinev and Hart 2006, Dinev et al. 2006) who suggest that the consumer simultaneously evaluates two sets of contrary factors: facilitators and inhibitors. Thus, when studying the adoption of controversial ITs, researchers should employ a net valence approach where they consider relevant and salient concerns as well as benefits.

2.1. Contextualization for Controversial ITs

Whetten (2009, p. 31) defines context as "the set of factors surrounding a phenomenon that exert some direct or indirect influence on it." Rousseau and Fried (2001, p. 1) outline that "contextualization entails linking observations to a set of relevant facts, events, or points of view that make possible research and theory that form part of a larger whole." While contextualization may require researchers to forgo parsimony and generalizability (Hong et al. 2014), it can have both subtle and powerful effects on research results (Johns 2006). When context is not understood, the person–situation interactions cannot be fully understood (Johns 2006), and findings may be incomplete and/or inconclusive (Whetten 2009). Additionally, context can help make research salient and relevant outside of the research community. Practitioners care about context because it can help solve practical problems as well as shape strategies and their implementation (Johns 2006, Lee and Baskerville 2003).

Hong et al. (2014) outline some approaches and guidelines for theorizing about information systems (IS) phenomena through contextualization. They indicate that there are two general approaches to incorporating context into theory development: (i) single-context theory contextualization, where well-established theories serve as a foundation from which constructs may be added or removed, and (ii) cross-context theory replication, where a theoretical model is replicated in different contexts and findings are consolidated by conducting a theory-grounded meta-analysis.

In our investigation, the former approach is followed, where well-established theories that balance benefits and concerns in determining attitude (e.g., net valence) are contextualized by incorporating appropriate constructs relevant to the controversial IT in question and its intended application and context of use. This incorporation can be conducted by adding contextual factors as antecedents to core theory constructs (where core theory constructs mediate the relationship between the contextual factors and endogenous variables), by adding contextual factors as moderators of core theory relationships, or by formulating context-sensitive versions of the core theory constructs (Hong et al. 2014). We employ two of these three approaches for contextualization. First, we seek to decompose the high-level core constructs of benefits and concerns into those that pertain to the context of a particular controversial IT. Second, we add contextual factors as antecedents of contextualized core theory constructs. According to Hong et al. (2014), the latter approach is the most common and allows the contextual variables to directly influence the underlying theory (Bagozzi 2007, Whetten 2009), which we also contextualize.

We propose that attitude toward a controversial IT is formed by contextualized benefits and concerns, which are in turn influenced by contextual characteristics. Attitude is chosen as an appropriate outcome variable as controversial technologies tend to have high individual involvement (Bredahl 2001). High individual involvement has strong links with values, which leads to strong attitudes (Thomsen et al. 1995, Schwartz 1992). Furthermore, attitudinal beliefs are particularly relevant in the consumer decision-making context (Brown and Venkatesh 2005) and for technologies not currently in common use, which is the case for our investigation. Attitude can also reflect the extent of satisfaction with a particular object or behavior (Oliver 1980, Teo et al. 2003).

To assess the utility of the above framework, we study its application to consumer acceptance of biometric identity authentication for banking transactions through ATMs.[1] Biometrics is the science of measuring human physiological or behavioral characteristics (Clodfelter 2010). Biometrics-based systems can be used for both identity recognition and authentication. Identity authentication answers the question, is the user who he or she claims to be? In this context, the system authenticates the identity of that person and makes a yes/no decision based on a one-to-one comparison of the newly scanned biometric data to a previously stored version (Jain et al. 2004). Identity recognition, by contrast, answers the question, who is the user? In this case, the newly acquired biometric information is compared to all available biometric data files in a database using a one-to-many comparison process (Prabhakar et al. 2003). We focus on using biometric information for identity authentication, as it is more accurate than recognition (Jain et al. 2004).

While the initial thrust toward the adoption of biometric tools for identity authentication originated from governments in their pursuit of introducing biometric-enabled travel documents, such as passports, other organizations, and the banking industry in particular, are showing considerable interest in biometrics' potential to unequivocally authenticate/identify individuals. Security is vital in the retail banking industry, which is constantly under the threat of fraud and security system breaches. Bank card–related fraud continues to result in significant losses for the retail banking industry, even after the introduction of the chip-and-PIN (personal identification number) system (Ennis 2012). ATMs are one of the most important banking entry points needing protection because of their high customer use (Ennis 2012). Banks are increasingly interested in new technologies that can address the security gaps in their ATM channel, which currently relies on the somewhat vulnerable card with chip-and-PIN system (Ennis 2012). However, before such technology can be widely deployed at ATMs, banks must fully understand the factors that shape consumers' acceptance of technologies, such as biometrics, in banking applications.

Despite the growing interest in the use of biometric identity authentication technology, empirical research on citizen/consumer acceptance is limited in terms of the number of studies conducted and the examination of antecedents that may influence attitudes and the ultimate adoption of this technology. The work of James et al. (2006) was one of the first efforts to examine consumer acceptance of biometrics. They developed a generalized adoption model across a wide variety of biometric devices and applications. Since then, a handful of papers have examined biometrics from various perspectives. For example, Clodfelter (2010) examined consumer acceptance of fingerprint authentication at point-of-sale in retail outlets; Morosan investigated user acceptance of biometrics with respect to air travel (Morosan 2012b), hotels (Morosan 2012a, c), and restaurants (Morosan 2011); Byun and Byun (2013) studied consumer acceptance of biometrics at ATMs, focusing on perceived consumer value; and Miltgen et al. (2013) looked at acceptance of biometrics in a driver's test context. Although these articles provide some insights into the complex understanding of consumer acceptance of biometric technologies, they do not specifically incorporate the appropriate contextual factors that could influence the adoption of biometrics.

To address this research gap, we first contextualize the core constructs of perceived benefits and concerns to the chosen domain (biometric identity authentication for banking transactions through ATMs) by carrying out a qualitative study involving 402 participants

(Study 1). Second, to determine the appropriate contextual factors as antecedents of the contextualized core constructs, we examine past relevant research in this area. Both these approaches for identifying context-specific factors (qualitative methods and the examination of extant relevant research) are identified and supported by Hong et al. (2014). Third, we develop a contextualized research model that is validated in a quantitative study involving 437 participants (Study 2).

3. Study 1: Understanding Perceived Benefits and Concerns of Biometric Identity Authentication

Despite extensive research on the technical aspects of biometric security technologies, there is limited research on consumer acceptance of biometrics (Clodfelter 2010, Miltgen et al. 2013). The beliefs of end users are important considerations when designing and implementing controversial ITs that employ highly personal digital identities (Jones et al. 2007). As such, we first conduct an exploratory qualitative investigation to better understand consumer beliefs (specifically, consumer perceptions of benefits and concerns) regarding biometric identity authentication technologies within a banking context.

3.1. Research Method and Sample

We recruited 402 participants (53.5% men) via a market research firm that had access to a broad pool of participants. Research has shown that age can be a major influence in how people perceive change, particularly with regard to technology acceptance, risk, and concerns associated with privacy and security (Gomez et al. 1986, Majchrzak and Cotton 1988, Wagner et al. 2010). Thus, we drew from a balanced sample of age groups to avoid bias in the results due to age. The breakdown of our sample by age is shown in Table A1 in Online Appendix A.

Data were gathered via an online survey. A description of fingerprint biometric authentication for ATM transactions was provided, and participants were asked the following three open-ended questions:

1. What do you feel are the benefits/advantages of using biometrics?
2. What concerns do you have using biometrics?
3. Please provide any other comments regarding the use of biometrics.

We used content analysis to analyze participants' responses in our qualitative study and analyzed data using a three-stage iterative process. In the first stage, we reviewed respondents' answers to the above questions and used open coding to identify shared characteristics and generate initial descriptive categories. The second stage consisted of scrutinizing the initially identified categories and integrating them into more centralized categories. In the final stage, the use of selective coding allowed the synthesis of these centralized categories into overriding themes (Strauss and Corbin 1990). In this investigation, one researcher conducted the first and second stages. The final stage was conducted through meetings and discussion among three IS research experts, where participant responses were reviewed for consistency and to build consensus.

3.2. Results

We used QSR NVivo to apply codes to responses, sort responses by code categories, organize code hierarchies, and help identify common themes. Following the first- and second-stage analyses of the grounded theory approach, we identified the following general categories as benefits of using biometric identity authentication in the context of ATM transactions (example comments pertaining to these categories are provided in Table A2 in Online Appendix A):

1. Increased security
2. Increased safety
3. Difficulty in reproduction of fingerprints
4. Deterrent to identity theft
5. I am the only one with access to my accounts
6. Less chance of theft from my accounts
7. Less chance of theft of my PIN/password
8. Less concern if I lose my card
9. Easier to use
10. No chance of forgetting your card
11. No PIN/password to remember
12. Convenience
13. Faster access to accounts

The third-stage analysis resulted in the synthesis of the 13 broad benefit categories into the following two overriding themes due to the commonalities identified:

(1) Account security (Items 1 through 8; mentioned by 201 participants)

(2) Convenience (Items 9 through 13; mentioned by 94 participants)

After the first- and second-stage analyses, the following general categories were identified as concerns about using biometric verification in the context of ATM transactions (example comments pertaining to these categories are provided in Table A3 in Online Appendix A):

1. How secure is my information from hackers/insiders?
2. My fingerprints can be copied
3. Increased possibility of identity theft
4. Inconvenience
5. Inability to share banking responsibilities with others
6. Reliability of the technology in terms of startup glitches, ongoing maintenance issues, and accuracy of the fingerprint reader due to dirt, grease, etc.
7. Slower access to accounts
8. What happens if my fingers are damaged, or if they become damaged?

9. What happens when I go overseas and they aren't using biometrics at ATMs?

10. The information is too private for any organization to have

11. Physical harm as thieves will now sever my fingers and/or hand to gain access to my account

12. Function creep—private information is shared beyond intended use either by corporations and/or the government

The third-stage analysis resulted in the synthesis of the above 12 categories into the following four recurring themes:

(1) Security concerns (Items 1 through 3; mentioned by 140 participants)

(2) Inconvenience (Items 4 through 9; mentioned by 77 participants)

(3) Privacy concerns (Items 10 and 12; mentioned by 176 participants)

(4) Physical harm (Item 11; mentioned by 38 participants)

Two graduate research assistants unaware of the study's purpose validated our categorizations and overriding themes. These coders were given a code book of the identified centralized categories for benefits and concerns of using biometric identity authentication at ATMs and were asked to code the participants comments. Cohen's kappa was calculated to assess the reliability of coding and validity of the data analysis. The kappa coefficients were 0.908 ($n = 411$) and 0.902 ($n = 536$) for the centralized benefits and concerns categories, respectively, indicating substantial agreement between the two coders (Landis and Koch 1977). Subsequently, the coders were given a code book of the identified overriding themes and asked to code the centralized categories into these themes. The coders were in complete agreement in grouping the benefit categories into the benefit themes as well as the concern categories into the concern themes.

It is noteworthy that security is identified as a benefit by half of the respondents while being simultaneously cited as a concern by almost 35% of the participants. However, when security is mentioned as a benefit, it is typically within the context of access to financial data (i.e., "only I can access my accounts," "the bank is sure it is me," etc.). When security is mentioned as a concern, it is typically within the context of the bank not having appropriate safeguards to protect the biometric data itself. From a security concern perspective, respondents were worried about the risk of thieves accessing their biometric data and gaining access to their financial information and assets: "Anyone could hack into the system and take information"; "I have concerns about fingerprints which I think can be copied"; "Somebody somehow getting my fingerprint to access my account"; and "Fingerprints left on ATMs may be lifted and used by those who know how." Respondents recognized that unlike PINs, biometric information cannot be changed if compromised through a security or privacy breach.

When examining convenience versus inconvenience, 23% of respondents mentioned the former as a benefit, while 19% mentioned the latter as a concern. However, unlike security in which respondents were discussing two different aspects, convenience and inconvenience appear to be more of a paradox in that participants are looking at opposite sides of the same issue. Convenience and inconvenience referred to facilitating the banking tasks for individuals. The benefits of convenience cited were typically related to (i) the increased ease in accomplishing banking tasks without having to remember PINs ("You can't forget your fingerprint"; "No PIN numbers to remember"; "It's one less password to forget") and (ii) faster service ("It would be a faster way to access my money"; "Fast, convenient, don't have to risk forgetting the PIN"). Respondents who expressed concerns about inconvenience stressed the inability to share banking responsibilities with others, as shown in the following example comments: "If I am sick and unable to go to the bank to get money, my partner would not be able to go for me"; "If needed, someone else cannot do your banking for you"; and "Personally, I allow my fiancée to access my bank account. Whoever has the free time that day takes both cards and pay cheques or withdrawals and runs to the bank for us both." Essentially, such concerns relate to the inability of customers to accomplish their banking more quickly (e.g., a delay due to being sick and not being able to share their bank card with a partner) or more easily (e.g., having to personally drive to the bank instead of just asking one's partner to do it on his or her way back from work on a given day). As such, the convenience benefit and inconvenience concern examine the same issues of being able to accomplish banking tasks "more quickly" and "more easily." Therefore, inconvenience is not included as a distinct concern in our investigation, as it is captured within perceptions of convenience.

Privacy was the most cited concern overall and for each age group in our sample, with a total of 176 respondents commenting on it. This confirms the finding in the literature that all generations value their privacy (Clarke 1999). Responses in this concern area included, "Privacy is important to all of us and by using this we are giving out way too much"; "I don't like the idea of someone having that much information about me"; "Biometrics is more secure but we have to make sure that our privacy and our rights remain protected at all cost"; and "I am concerned about misuse of the technology and the potential of loss of privacy."

Finally, of lesser concern among all respondents was physical harm. Actual physical harm (i.e., severing of fingers by criminals to gain access to bank accounts)

was cited as a concern by 38 respondents. Some of the respondents stated: "I would also be concerned about people attacking me, cutting off my finger, and using it to access my account. Then I've lost money and a finger." And, "Please be aware that criminals will use whatever means they have to in order to steal, and therefore they may cut off fingers to gain access, etc." This represents a lack of understanding of biometric device functioning, as most systems require living flesh to operate properly. Given the small numbers associated with this concern compared to privacy and security concerns (38 versus 176 and 140, respectively), it is not included as a distinct concern construct in our investigation.

The results of our qualitative study indicate that in the context of biometric identity authentication at ATMs, the most salient perceived benefits are account security and convenience, and the most salient perceived concerns are privacy concerns and security concerns. These results inform the next strand of our research investigation, where we develop and validate a model to understand users' attitudes toward using biometrics for identity authentication.

4. Hypotheses

As indicated earlier, in studying acceptance of controversial technologies, attitude is a more appropriate dependent variable to use than behavioral intention. As outlined in Section 2, we propose that attitude is determined by perceived benefits and perceived concerns, leading to the following general hypotheses:

Hypothesis 1. *Benefits from using controversial ITs will positively influence attitude toward such technologies.*

Hypothesis 2. *Concerns from using controversial ITs will negatively influence attitude toward such technologies.*

Based on these general hypotheses, we advance specific hypotheses for each contextualized benefit and concern related to the use of the controversial IT of biometric identity authentication at ATMs as determined from our qualitative analysis, namely, account security and convenience as benefits and privacy and security as concerns.

Account Security. Account security is the belief that the technology (biometric identity authentication) will keep one's bank account safe from the threat of unauthorized access. Technology threat avoidance theory (TTAT; Liang and Xue 2009) postulates that when IT users are faced with a threat, they first assess the likelihood and potential impact of that threat on their well-being and then assess potential coping mechanisms to minimize or avoid that threat. It is well documented that debit and credit card fraud, including their use at ATMs (an IT), is a top concern for consumers (Sakharova 2012). Thus, consumers recognize the existence of a threat to their financial well-being due to security weaknesses in the current way they access their bank accounts through ATMs (i.e., bank card and PIN). These perceptions were substantiated in a study that showed increased security as one of the perceived consumer benefits in using fingerprint identity authentication at ATMs (Byun and Byun 2013). Thus, consumers are likely to view biometric identity authentication at ATMs as an IT precaution to cope with the threat of fraudulent access to their bank accounts by providing a higher level of assurance that no one else can access their bank accounts but them. This perception was evidenced through participants' comments in our qualitative study (Study 1) about biometric identity authentication such as "more secure knowing that only you can access your bank account." This added assurance against the threat of unauthorized bank account access should positively influence consumers' attitudes toward such technologies. As such, we hypothesize the following:

Hypothesis 1A. *Bank account security due to using biometric identity authentication technology to access one's bank account*(*s*) *through ATMs will positively influence attitude toward such technology.*

Convenience. Convenience is the belief that the technology (biometric identity authentication) will make the task of accessing one's bank account through an ATM quick and easy. As mentioned previously, according to TTAT, consumers seek assurance against the threat of unauthorized bank account access. Utilizing current ATM authentication methods of bank cards and PINs requires customers to remember their PINs and to change these PINs on a regular basis to strengthen their assurance against that threat. By contrast, biometric identity authentication not only provides stronger assurances but also is easier to use (i.e., no longer having to remember or change PINs) and faster to use than current authentication methods. Such perceptions were evidenced through comments in our qualitative study such as, "There are no numbers to remember. All you have to do is put your index finger on the screen." It is anticipated that the convenience afforded through this approach to identity authentication at ATMs will positively influence consumers' attitudes toward such technologies. As such, the following hypothesis is advanced:

Hypothesis 1B. *Convenience due to using biometric identity authentication technology to access one's bank account*(*s*) *through ATMs will positively influence attitude toward such technology.*

Privacy and Security Concerns. We employ a definition of privacy concerns from Pavlou et al. (2007, p. 113): "consumer beliefs about a seller's inability

and[/or] unwillingness to protect her personal information from improper use, disclosure to third parties, and secondary use without the buyer's consent." We define security concerns as consumer beliefs that the holder of personal information will not have the "technical guarantees that ensure the legal requirements and good practices with regard to privacy will be effectively met" (Flavián and Guinalíu 2006, p. 604). It is important to note that in the current context, privacy and security concerns relate to the biometric information itself, rather than concerns with the privacy and security of financial information/bank accounts.

In the context of biometric technologies, Al-Harby et al. (2008) found that privacy and security reservations were obstacles to adoption of this controversial technology. Consumers carefully compare the perceived risks against the anticipated benefits of using such technologies. While consumers may appreciate that biometric identity authentication is a more secure way of accessing their bank accounts (as detailed in Hypothesis 1A), they are simultaneously concerned about giving away such private and personal information as well as the security measures employed to keep this information safe. As evidenced from our qualitative study, consumers are concerned that banks would be in possession of such private information (e.g., "Gives banks too much personal information, and I am not comfortable with the notion") and that this information may be used beyond its intended purpose (e.g., "Could law enforcement subpoena their records? Could they fall into other hands?"). Additionally, consumers worry that if their biometric data were hacked or copied due to inadequate security, the consequences would be much more dire than a simple card and PIN being compromised (e.g., "If identity theft occurred, it would be far worse than now"). While one can replace a card and PIN, one cannot replace a compromised fingerprint. As such, the concerns stemming from the privacy and security of biometric information would negatively influence consumers' attitudes toward such technologies. Thus, we hypothesize the following:

Hypothesis 2A. *Privacy concerns from using biometric identity authentication technology to access one's bank account(s) through ATMs will negatively influence attitude toward such technology.*

Hypothesis 2B. *Security concerns from using biometric identity authentication technology to access one's bank account(s) through ATMs will negatively influence attitude toward such technology.*

The second set of general hypotheses examines the influence of contextual characteristics on perceived benefits and concerns.

Hypothesis 3. *Contextual characteristics of using controversial ITs will influence perceptions of benefits of such technologies.*

Hypothesis 4. *Contextual characteristics of using controversial ITs will influence perceptions of concerns of such technologies.*

Rather than examining a broad range of contextual characteristics, we focus on those factors where a bank may influence change (i.e., through their initiatives, education, and implementation). By focusing on such elements, our results can provide tangible and actionable guidelines for practitioners in addition to advancing academic knowledge. Drawing from extant literature on controversial technologies, biometrics, and privacy, we identify three factors specific to our context of investigation where banks may influence change: (1) familiarity, (2) trust in the bank, and (3) perceived control.

Familiarity. When a new technology is introduced, people are naturally ignorant of what it is and/or what it does. Familiarity with a new technology develops as people learn about or interact with it (Yoon and Rolland 2012). In our context of biometric identity authentication, banks can influence the familiarity of their customers with this technology by providing information/education, helping to answer any questions that arise, and providing customers opportunities to interact with the technology.

According to Rogers' (2003) diffusion of innovation theory, innovation acceptance goes through five stages: knowledge, persuasion, decision, implementation, and confirmation. Given that biometric identity authentication is a relatively new innovation, most consumers are at the knowledge stage, where there is general awareness that the innovation exists. Having sufficient knowledge (i.e., familiarity) about a new innovation shapes an individual's beliefs about its utility (i.e., benefits) (Straub 2009), which is critical to moving to the next stage of acceptance (i.e., persuasion[2]). Hence, consumers who have higher familiarity with biometric technologies for identity authentication will be in a better position to realize the benefits of account security and convenience that accrue from the use of this technology at ATMs. Thus, we hypothesize the following:

Hypothesis 3A. *Familiarity with biometric technologies will positively influence one's perceptions of bank account security when bank accounts are accessed through ATMs using biometric identity authentication.*

Hypothesis 3B. *Familiarity with biometric technologies will positively influence one's perceptions of convenience when bank accounts are accessed through ATMs using biometric identity authentication.*

Trust in the Bank. Trust refers to beliefs or perceptions one holds about another party (such as their integrity, benevolence, ability, and predictability; Gefen et al. 2003). Banks can influence the trust their customers

have in them through the development of positive corporate image via means such as advertising and marketing campaigns, clear and visible privacy policies, and website design (Flavián et al. 2005, Yousafzai et al. 2003, Hassanein and Head 2007).

If customers have a high level of trust in their bank, they will believe that when their bank implements a new technology, it will be both competent (has the ability) and willing (has the benevolence and integrity) to take the necessary steps to maximize the potential benefits while reducing the potential concerns associated with the use of this technology. These necessary steps include the choices made by the bank regarding hardware and software associated with the technology as well as the processes put in place for its use. The quality of identity authentication systems is generally assessed by their ability to minimize two types of errors: false accepts and false rejects (Jain et al. 2004). This is usually a trade-off, and an appropriate balance is established based on the specific application at hand (Jain et al. 2004). False accept errors refer to the system erroneously allowing an unauthorized user to access a bank account illegitimately, while false reject errors refer to the failure of the system to allow an authorized (legitimate) user access to their bank account. For identity authentication at ATMs, false rejects would occur when the bank machine does not recognize legitimate fingerprints due to a technical failure or external factors such as humidity, for example. In the context of the current investigation, false accepts would reduce account security, while false rejects would reduce convenience. Customers who trust their bank are likely to believe that the bank will minimize these two types of errors, resulting in higher account security (through minimizing false positive errors) and higher convenience (through minimizing false negative errors). As such, we hypothesize the following:

Hypothesis 3C. *Trust in one's bank will positively influence one's perceptions of bank account security when bank accounts are accessed through ATMs using biometric identity authentication.*

Hypothesis 3D. *Trust in one's bank will positively influence one's perceptions of convenience when bank accounts are accessed through ATMs using biometric identity authentication.*

In the same vein, customers that trust their bank are likely to believe that the bank will take appropriate actions to minimize concerns that may arise from the use of a new technology that it implements. In the context of biometric identity authentication at ATMs, customers that trust their bank would likely believe that the bank would implement provisions (through robust technologies and processes) to ensure the security of their biometric information against unauthorized access. Similarly, they would believe that their bank would keep this personal information private and not share it with third parties without their explicit consent. Hence, we argue that trust in one's bank could play a role in reducing consumers' privacy and security concerns toward surrendering or sharing their biometric information with their bank. Thus, we hypothesize the following:

Hypothesis 4A. *Trust in one's bank will negatively influence perceptions of privacy concerns when bank accounts are accessed through ATMs using biometric identity authentication.*

Hypothesis 4B. *Trust in one's bank will negatively influence perceptions of security concerns when bank accounts are accessed through ATMs using biometric identity authentication.*

Perceived Control. In the context of personal information, perceived control is the extent to which a consumer feels that he or she has influence over their personal information that another party (individual, merchant, institution, government, etc.) possesses (Bateson and Hui 1992, Arcand et al. 2007). For biometric identity authentication, control is conceptualized as the personal control one has over his or her biometric data (e.g., the more that an individual has possession of his or her biometric data, the greater the sense of perceived control over this sensitive information). Control over personal information is of central importance in examining consumer attitudes toward controversial ITs (Frewer et al. 2004). As with familiarity and trust in the bank, banks can influence the perceived control customers have over their biometric data through the implementation strategy of biometric identity authentication technology (such as allowing the customer to retain full or partial ownership of their sensitive biometric information).

Prior research has shown that individuals who perceive a greater degree of control over the private information they share via IT have fewer privacy concerns (Bandyopadhyay 2011, Xu et al. 2011, Xu 2007). In the context of biometric identity authentication, when individuals have possession of their personal biometric information, they are fully aware of how that information is used and have a higher sense of control over this information, and consequently have fewer privacy concerns compared to when another party (i.e., the bank) has possession of this information. By extension, and as security is a critical element of privacy, by having possession of their biometric information and the full knowledge of how this private information is secured, customers will likely have fewer security concerns compared to when another party has possession of this information. Furthermore, a recent study assessing the perceptions of adults in the United States regarding their personal health information revealed that they

were less likely to share this information (because of privacy and security concerns) if they felt that they had low control over how their medical records were collected and used (Agaku et al. 2014). Thus, we hypothesize the following:

Hypothesis 4C. *Perceived control over one's biometric information will negatively influence perceptions of privacy concerns when bank accounts are accessed through ATMs using biometric identity authentication.*

Hypothesis 4D. *Perceived control over one's biometric information will negatively influence perceptions of security concerns when bank accounts are accessed through ATMs using biometric identity authentication.*

5. Study 2: Validating the Contextualized Research Model

We employed a survey to quantitatively validate our proposed research model. While participants did not have direct experience with biometric identity authentication technology, the experiment was framed in a familiar setting of using an ATM to access one's bank account. Similarly, fingerprints were used as the biometric for identity authentication because of their familiarity in general media across various applications.

5.1. Research Method and Sample

Individuals in our sample were recruited through a market research firm with access to a broad pool of participants. To participate in the study, participants had to (1) live in the United States, (2) be over the age of 18, (3) not work for a bank, (4) have an active bank account, and (5) use ATMs. Since banking systems may differ greatly across countries, one country for investigation was chosen to prevent the potential confounding effect of diverse banking systems. We chose the United States as our context of study as this market is estimated to host in excess of 7,000 banks of various sizes (Baumann et al. 2012), which would result in variability in consumer trust perceptions of their banks.

Participant demographics are summarized in Table B1 in Online Appendix B. This was a balanced stratified sample by the U.S. age demographic (over the age of 18). To incentivize participation, the market research firm used sweepstakes prize pools. After completing the survey, a respondent could enter his or her email address for a chance to win one of five monthly prizes of $1,000. The overall response rate could not be calculated, as the market research firm used in this investigation was not able to provide these data. From the 439 completed surveys, two were removed because of both univariate and multivariate outlier issues following box-plot (Meyers et al. 2006) and Mahalanobis distance analyses. Thus, the total sample size for this investigation was 437.

As indicated earlier, the development of context-specific theory is deemed an important frontier advancing IS research (Venkatesh and Bala 2008). From the contextual independent variables identified (familiarity, trust in the bank, and perceived control), banks can vary how they implement the characteristic of biometric data control. For example, a bank may choose to store a consumer's complete biometric information or may store only half of the biometric identifier while the consumer retains the other half on a smart card. As such, the former implementation should result in less perceived customer control (as the bank holds all of the biometric data), while the latter implementation should result in more perceived customer control (as the bank holds only part of the biometric data, which alone are useless unless they are paired with the data stored on the consumer's smart card). Thus, perceived control was selected for manipulation in our investigation.

In the case of biometric identity authentication, most applications are not yet widely used and/or implemented and as a result have not been experienced firsthand by consumers. Therefore, scenario-based research is appropriate to examine the effects of situational implementation options (Sheng et al. 2008). In this study, we created two implementation scenarios to experimentally manipulate perceived control. A between-subjects design was used in which respondents were given only one of the two scenarios (Keppel 1991). Thus, respondents were randomly assigned to one of the two scenarios. The randomization was performed with computer scripting involving a random number generator while observing age and group quotas to obtain a properly stratified sample. Respondents were unaware of having been placed in a group. The sample sizes for the bank control (low perceived user control) and shared control (high perceived user control) implementation scenarios were 203 and 234, respectively. The exact wording of the two implementation scenarios (bank control and shared control) used in the current investigation is provided in Online Appendix B. By using the scenario method to manipulate perceived control, we are able to ascertain which control context for the proposed future technology will have a higher degree of acceptance for consumers (Sheng et al. 2008, Bria et al. 2001).

Participants first answered some qualifying questions. As indicated above, if they were under the age of 18, worked for a bank, did not have an active bank account, or did not use an ATM, they were thanked for their time and did not continue with the survey. Following the qualifying questions, participants had to complete a consent form before proceeding further. Next, participants were asked about their familiarity with biometrics technology, their trust in their bank, and their perceptions of biometrics' efficacy in keeping their bank accounts secure. Subsequently, each

respondent was presented with either the bank control or the shared control scenario (shown in Online Appendix B). After reading the scenario, participants were asked to respond to items for perceived control, convenience, privacy concerns, security concerns, and attitude. Finally, participants were asked questions pertaining to their demographics.

5.2. Results[3]

Structural equation modeling (SEM) was conducted using partial least squares (PLS), which is a component-based approach. We examined the normality of our data (using statistical approaches of skewness and kurtosis as well as graphic approaches by examining histograms and normal probability plots) and found there were indications of nonnormal data for our constructs. PLS is robust to deviations from normality (Chin 2010), thus validating our choice of this SEM approach.

Measurement Model Assessment. The constructs used in this study were adapted from instruments developed and validated in prior studies. Table B2 in Online Appendix B shows the wording of all of the construct items and their sources. Thus, content validity was established through literature review (Straub 1989). Account security was operationalized through the response efficacy scale (Norman et al. 2003), which stems from protection motivation theory (Rogers 1975). In our context, response efficacy refers to the belief that the technology (i.e., biometric identity authentication technology) will effectively reduce the risk of one's bank account being compromised (i.e., by increasing account security). Convenience was operationalized through a transaction convenience scale adapted from Colwell et al. (2008).

We used a PLS approach to confirmatory factor analysis (CFA) to assess the psychometric properties of the multi-item scales. This approach is well suited to studies where scales have been used and validated in prior work. We assessed convergent and discriminant validity by examining the factor loadings to ensure that items load cleanly on their related factors and do not cross-load on other factors. For convergent validity, all indicators should load most highly on their own theoretically assigned construct and at a minimum threshold of 0.70. As shown in Table B3 in Online Appendix B, two items (SC2 and TRUST4) did not meet this threshold and were removed from subsequent analysis. Table B4 in Online Appendix B shows that the loadings for all scale items were significant at $p < 0.001$.

From Table 1, the composite reliabilities of all constructs exceeded 0.80 (the lowest being 0.89 for trust), and the Cronbach's alphas exceeded 0.70 (the lowest being 0.83 for trust). The square roots of the average variance extracted (AVE) are shown along the diagonal in bold and exceed the 0.71 threshold (the lowest being 0.81 for trust). Thus, all conditions for convergent validity were met (see Fornell and Larcker 1981).

In the analysis of discriminant validity, the point is to assess how variables in each distinct causal stage of the model behave. What is not important is how items may or may not cross-load across these stages. For example, if there is a posited causal link between two constructs, then it is expected that measures of the independent construct may highly correlate with those of the dependent construct (Straub et al. 2004). Thus, in our proposed model, we are interested in testing the cross-loadings of familiarity, trust in the bank, and perceived control (first causal stage) and testing the cross-loadings of account security, convenience, privacy concerns, and security concerns (second causal stage). The complete matrix of cross-loadings is provided in Table B3 in Online Appendix B. When using the PLS CFA method to examine discriminant validity, Gefen and Straub (2005) recommend that the measurement item loadings on their assigned latent variables should be an order of magnitude larger than their

Table 1. Scale Properties and Correlation Matrix

			Interconstruct correlations							
Construct	α-value	Comp. rel.	1	2	3	4	5	6	7	8
1. *ATT*	0.97	0.98	**0.96**							
2. *ASEC*	0.98	0.98	0.59***	**0.97**						
3. *CONV*	0.94	0.97	0.72***	0.40***	**0.97**					
4. *PC*	0.95	0.96	−0.51***	−0.28***	−0.27***	**0.89**				
5. *SC*	0.93	0.96	−0.81***	−0.51***	−0.61***	0.55***	**0.94**			
6. *FAM*	0.87	0.92	0.23***	0.26***	0.18***	−0.06	−0.16***	**0.89**		
7. *TRUST*	0.83	0.89	0.36***	0.38***	0.29***	−0.16***	−0.38***	0.12*	**0.81**	
8. *PCTRL*	0.96	0.97	0.72***	0.53***	0.56***	−0.39***	−0.72***	0.16***	0.37***	**0.92**

Notes. Comp. rel., Composite reliabilities; ATT, attitude; ASEC, account security; CONV, convenience; PC, privacy concerns; SC, security concerns; FAM, familiarity; TRUST, trust in bank; PCTRL, perceived control. The diagonal elements (in bold) represent square roots of AVE for those constructs.

*$p < 0.05$; ***$p < 0.001$.

loadings on other variables (in its causal stage), indicating specifically that this difference should be at least 0.10. As shown in Table B3 in Online Appendix B, this criterion is met.

We also assessed discriminant validity between constructs, per Fornell and Larcker (1981), where the correlations between any two constructs should be lower than the square root of the average variance shared by items within a construct. As shown in Table 1, this criterion is satisfied. Table 1 also shows that the bivariate correlations were in the expected directions, providing preliminary support for our hypothesized main effects.

Table 1 reveals that some of the interconstruct correlations are rather high (above 0.7), which raises a potential multicollinearity issue. However, multicollinearity is an issue when more than two predictors correlate very strongly, and not when correlations exist between predictors and a dependent variable (Meyers et al. 2006, Straub et al. 2004). The highest interconstruct correlation for variables within the same causal stage in Table 1 is below 0.7 (0.61 for security concerns and convenience). As an additional assessment, we conducted a multicollinearity test for all variables in the model using SPSS. All variance inflation factors were less than 2.5, and all tolerance values were greater than 0.40, which are the thresholds recommended by Allison (1999). We conclude that multicollinearity is not a problem and discriminant validity has been met for our data sample.

Manipulation Check. To test whether the two scenarios used in our experiment were effective in manipulating perceptions of perceived control, we conducted a manipulation check using analysis of variance in SPSS 20.0 for the perceived control scale used by Xu et al. (2011). The test indicated that the two scenario groups were significantly different in terms of their perceived control ($F = 8.544; p = 0.004$). Therefore, the experimental scenarios used were successful in manipulating the perceived control of participants in our investigation, where respondents perceived more control in the shared control scenario (mean = 4.84) compared to the bank control scenario (mean = 4.38).

Structural Model Assessment. The structural model, depicted in Figure 1, was evaluated using SmartPLS version 3.2.0 (Ringle et al. 2005). Approximately 77% of the variance in attitude toward using biometric technology for identity authentication at ATMs is accounted for by the variables in the model ($R^2 = 0.776$). The R^2 of all endogenous constructs in the model exceeded the 10% benchmark recommended by Falk and Miller (1992). Additionally, we calculated the goodness of fit (GoF) of the model (Tenenhaus et al. 2005, Esposito Vinzi et al. 2010), which assesses the overall prediction performance of the model (both measurement and structural levels). The absolute GoF value for the proposed model is 0.543. Absolute GoF values of 0.1, 0.25, and 0.36 are considered low, medium, and high fit, respectively (Tenenhaus et al. 2005). As such, the absolute GoF of our proposed model indicates a high fit.

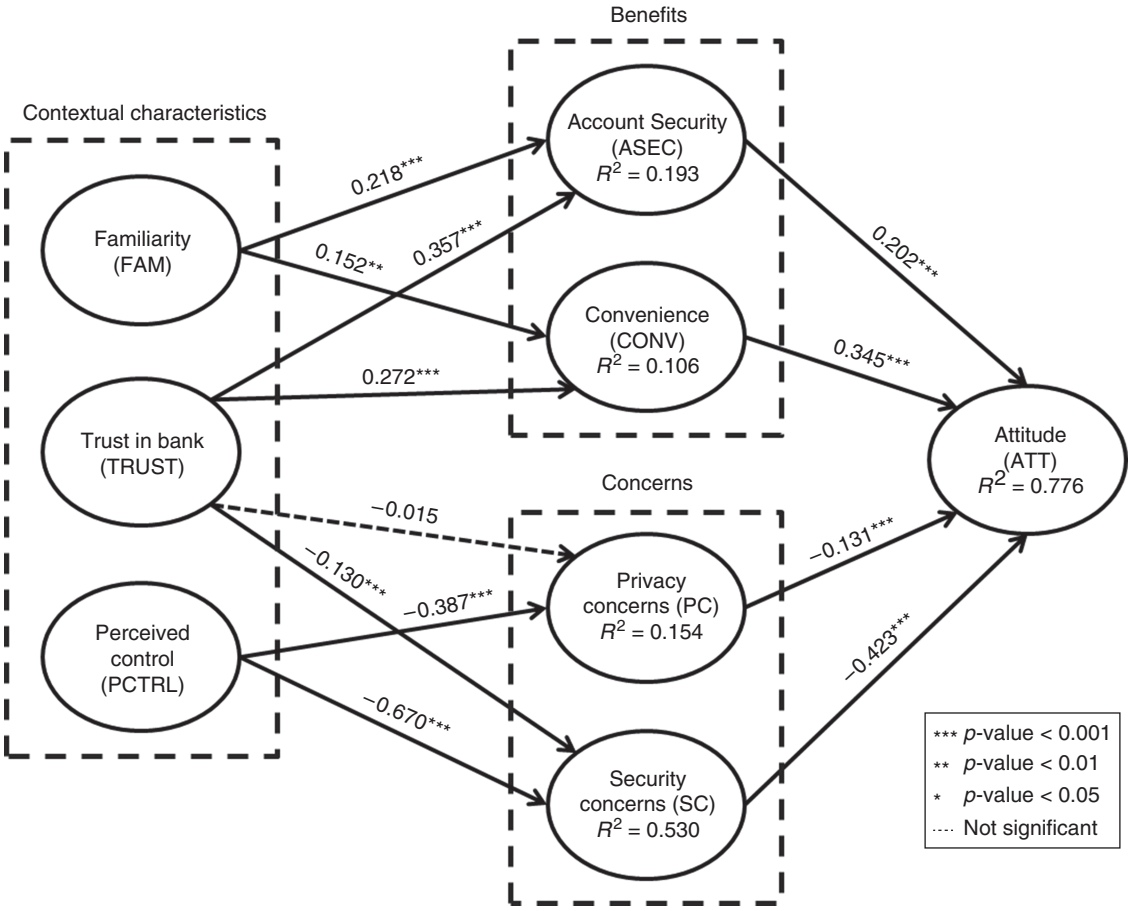
Having found support for the validity of our proposed model, we conducted a post hoc analysis to explore possible impacts of demographic control variables. Age, gender, income, and education were examined for their possible effects on the endogenous constructs in the research model. One controlled model was created for each control variable by adding the variable with connecting paths to all endogenous constructs in the model. The R^2 values for each endogenous variable were compared in the uncontrolled and controlled models (Chin 1998). Per Chin (1998, p. 316), "the change in R-squares can be explored to see whether the impact of a particular independent [variable] on a dependent [variable] has substantial impact." From this analysis, only gender had a small effect on convenience and security concerns ($f^2 = 0.026$), whereby females had higher security concerns compared to males. Thus, we conclude that demographic variables did not have any substantial effect on our research model.

In a further post hoc analysis, we examined the mediation effects. There are four constructs in our model (account security, convenience, privacy concerns, and security concerns) that are proposed to mediate the effects between contextual independent variables and attitude. Table B5 in Online Appendix B shows the results of our Sobel tests of mediation. Privacy concerns' mediation between trust in the bank and attitude was not tested, as this was a nonsignificant relationship in our model. The relationship between familiarity and attitude is shown to be fully mediated through account security and partially mediated through convenience. Relationships between trust and attitude and perceived control and attitude are partially mediated through appropriate benefits and concern.

6. Discussion

From a scientific perspective, this research makes important contributions by (i) leveraging net valence theories as well as extant controversial technologies and context of use literature to develop and validate a contextualized general research framework for understanding consumer attitudes toward controversial ITs and (ii) demonstrating the utility of this contextualized framework to understand consumer acceptance of a particular controversial IT (biometric identity authentication). The proposed framework is general in nature and represents a viable lens for examining consumers' attitudes toward any controversial IT given the simultaneous evaluation of perceived benefits and perceived concerns that ultimately shapes consumers' attitudes

Figure 1. Structural Model Results



Notes. ATT, Attitude toward adopting biometric identity authentication technology at ATMs; ASEC, perceived efficacy of biometric identity authentication technology for keeping one's bank account safe; CONV, convenience of biometric identity authentication technology at ATMs; PC, perceived privacy concerns with using biometric identity authentication technology at ATMs; SC, perceived security concerns with using biometric identity authentication technology at ATMs; FAM, perceived familiarity with biometric identity authentication technologies; TRUST, trust in one's bank; PCTRL, perceived personal control over ones biometric data.

toward these ITs. Thus, while the proposed contextualized general framework was subsequently developed into a more specific model that examined the acceptance of biometric identity authentication for financial transactions at ATMs by banking customers, it could be adapted to assess a variety of other context-specific applications involving controversial ITs.

Examining contextual factors and developing context-specific theories is important to the advancement of research in IS (Orlikowski and Iacono 2001, Venkatesh and Bala 2008, Hong et al. 2014). Extant literature on biometric adoption is lacking in this regard. The two-level contextualization approach we employed provides a deeper understanding of the specific factors that could influence the acceptance of this emerging controversial IT in a particular context of use. For biometric identity authentication at ATMs, we identified the core attitudinal antecedents of perceived benefits as increased account security and convenience, and of perceived concerns as privacy and security concerns. We also identified three independent contextual factors with potential impact on the above core attitudinal antecedents. Familiarity and trust in the bank were found to positively affect the perceived benefits of account security and convenience. Additionally, trust in the bank was found to reduce security concerns, while perceived control was found to lessen both privacy and security concerns. This latter result answers the call of Smith et al. (2011) in their interdisciplinary review of information privacy research for researchers to pay more attention to understanding antecedents of privacy concerns. Furthermore, our validated model demonstrates that the positive effect of perceived benefits (account security and convenience) on attitude is countered by the negative influence of the perceived concerns (privacy concerns and security concerns) associated with this controversial IT. This net valence approach is analogous to Culnan and Armstrong's (1999) *privacy calculus*. Our current

investigation extends this calculus through the addition of the distinct security concerns construct.

From a practitioners' perspective, our general framework demonstrates the importance of considering that consumers go through a net valence analysis when contemplating the adoption of a controversial IT. Identifying the specific benefits and concerns that consumers associate with a particular controversial IT is therefore critical for organizations as they contemplate the rollout of that technology, as is identifying the specific contextual factors that might influence consumers' perceptions of these benefits and concerns.

Our context-specific model, which focuses on the use of biometric identity authentication technology at ATMs, provides banking executives with specific and actionable strategies for enhancing the implementation, adoption, and use of this technology. The significant negative influences of privacy concerns and security concerns on attitude suggest that the threat of biometric information being compromised, either inadvertently or intentionally, is an important issue for consumers. Banks considering employing biometric identity authentication should therefore target their marketing campaigns at educating consumers on the superiority of biometric technologies relative to other forms of identity authentication (i.e., increased account security). Strengthening the perceptions of perceived benefits may, in turn, help counteract some perceived privacy and security concerns for consumers in a net valence approach, resulting in a more positive attitude toward adopting this technology. In addition, they should have clear provisions in place for safeguarding the security and privacy of consumers' biometric information and ensure that their consumers are aware of such provisions.

Additionally, control over ones biometric information was found to attenuate privacy concerns, while security concerns and trust in the bank were found to attenuate security concerns, suggesting that (i) increasing consumers' level of trust in financial institutions could mitigate security concerns directly (and perhaps privacy concerns indirectly since security is a necessary condition for privacy) such that consumer attitudes toward biometric identity authentication may be enhanced, and (ii) adding an element of customer control in biometric identity authentication would attenuate both types of concerns. As demonstrated in our investigation, a customer's perception of control can be directly and significantly manipulated by executing a shared biometric information implementation (as per our shared control scenario). Hence, banks considering rolling out a biometric identity authentication application can effectively utilize a shared control implementation to help lessen the concerns of their customers, and thereby create more positive attitudes toward this technology. While consumers can have unwavering trust in their financial institution, mistakes can still happen despite proper due diligence. Control can be analogous to a warranty when purchasing a new car. While consumers trust the manufacturer to build a high-quality car, they appreciate that mistakes can still happen and that the warranty adds an extra layer of protection and comfort. Similarly, providing shared biometric information control to banking customers can provide an extra layer of protection and comfort (thus reducing concerns), regardless of the amount of trust the customer may have in their financial institution.

7. Conclusion

In summary, this research is an important step in developing a general acceptance framework that can be contextualized as necessary to examine a variety of controversial ITs. While the findings from the specific model we empirically tested are a valuable step in determining consumer acceptance of fingerprint biometrics for identity authentication at ATMs, there are many other contexts and applications as well as a variety of biometrics to be explored. Given the nature of controversial ITs, and the sometimes visceral responses they illicit, it seems disingenuous to suggest that a generalizable model will be developed that can be applicable to all contexts, even within a specific controversial technology. The context in which the controversial IT is introduced and/or deployed will undoubtedly play a vital role in shaping consumers' attitudes such that results may differ when looking at introducing different biometrics in various applications and contexts. Nevertheless, as Johns (2006) points out, examining context adds a richness and robustness that can be lost when one's focus is generalizability, and there is always the chance that applying generalizable findings may lead to incorrect decisions and actions because the findings are, in actuality, not generalizable to the specific context at hand.

A search of popular media reveals an exhaustive number of recent articles discussing the ongoing global deployment of controversial ITs for a variety of purposes. What is also notable is the growing discontent among concerned consumers. Looking at biometric authentication systems, their existing and proposed deployments across a variety of applications in both the public and private sector are generating a backlash among those that are being enrolled without prior consultation or education. We hope that the research presented here is an important step toward understanding why, and in what contexts, individuals will or will not accept controversial ITs in general and, in the case of biometric identity authentication technology in particular, establishing some common ground and consensus between those that wish to deploy biometrics and those whom it affects.

Acknowledgments

The authors thank the senior editor and the anonymous reviewers for their constructive comments and guidance.

Endnotes

[1] Also known as automated banking machines (ABMs).

[2] This persuasion stage forms an individual's attitude toward the innovation in that being positively persuaded reflects a favorable attitude, while being negatively persuaded reflects an unfavorable attitude (Rogers 2003, Herie and Martin 2002).

[3] Common method bias did not impact our results, as shown in Online Appendix B.

References

Agaku IT, Adisa AO, Ayo-Yusuf OA, Connolly GN (2014) Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *J. Amer. Medical Informatics Assoc.* 21(2):374–378.

Al-Harby F, Qahwaji R, Kamala M (2008) The feasibility of biometrics authentication in e-commerce: User acceptance. Nunes MB, Isaías P, Ifenthaler D, eds. *Proc. IADIS Internat. Conf. WWW/Internet* (IADIS, Freiburg, Germany), 527–531.

Allison PD (1999) *Multiple Regression: A Primer* (Pine Forge Press, Thousand Oaks, CA).

Arcand M, Nantel J, Arles-Dufour M, Vincent A (2007) The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Inform. Rev.* 31(5):664–681.

Bagozzi RP (2007) The legacy of the technology acceptance model and a proposal for a paradigm shift. *J. Assoc. Inform. Systems* 8(4):244–254.

Baker EW, Al-Gahtani SS, Hubona GS (2010) Cultural impacts on acceptance and adoption of information technology in a developing country. *J. Global Inform. Management* 18(3):35–58.

Bandyopadhyay S (2011) Online privacy concerns of Indian consumers. *Internat. Business Econom. Res. J.* 10(2):93–100.

Bateson JEG, Hui MK (1992) The ecological validity of photographic slides and videotapes in simulating the service setting. *J. Consumer Res.* 19(2):271–282.

Baumann C, Hamin H, Tung RL (2012) Share of wallet in retail banking: A comparison of Caucasians in Canada and Australia vis-à-vis Chinese in China and overseas Chinese. *Internat. J. Bank Marketing* 30(2):88–101.

Bredahl L (2001) Determinants of consumer attitudes and purchase intentions with regard to genetically modified foods—Results of a cross-national survey. *J. Consumer Policy* 24(1):23–61.

Bria A, Gessler F, Queseth O, Stridh R, Unbehaun M, Wu J, Zander J (2001) 4th-generation wireless infrastructures: Scenarios and research challenges. *IEEE Personal Comm.* 8(6):25–31.

Brown SA, Venkatesh V (2005) Model of adoption of technology in households: A baseline model test and extension incorporating house-hold life cycle. *MIS Quart.* 29(3):399–426.

Byun S, Byun S-E (2013) Exploring perceptions toward biometric technology in service encounters: A comparison of current users and potential adopters. *Behav. Inform. Tech.* 32(3):217–230.

Cazier JA, Jensen AS, Dave DS (2008) The impact of consumer perceptions of information privacy and security risks on the adoption of residual RFID technologies. *Comm. Assoc. Inform. Systems* 23(1):235–256.

Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. Yang G, ed. *Proc. 2012 Internat. Conf. Comput. Sci. Electronics Engrg.*, Vol. 1 (IEEE Computer Society, Los Alamitos, CA), 647–651.

Chin WW (1998) The partial least squares approach for structural equation modeling. Marcoulides GA, ed. *Modern Methods for Business Research* (Lawrence Erlbaum, Mahwah, NJ), 295–336.

Chin WW (2010) How to write up and report PLS analyses. Esposito Vinzi V, Chin WW, Henseler J, Wang H, eds. *Handbook of Partial Least Squares: Concepts, Methods and Applications* (Springer, Berlin Heidelberg), 655–690.

Clarke R (1999) Internet privacy concerns confirm the case for intervention. *Comm. ACM* 42:60–67.

Clodfelter R (2010) Biometric technology in retailing: Will consumers accept fingerprint authentication? *J. Retailing Consumer Services* 17:181–188.

Colwell SR, Aung M, Kanetkar V, Holden AL (2008) Toward a measure of service convenience: Multiple-item scale development and empirical test. *J. Services Marketing* 22(2):160–169.

Culnan MJ, Armstrong PK (1999) Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organ. Sci.* 10(1):104–115.

Culnan MJ, Bies R (2003) Consumer privacy: Balancing economic and justice considerations. *J. Social Issues* 59(2):323–342.

Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Inform. Systems Res.* 17(1):61–80.

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. *Eur. J. Inform. Systems* 15:389–402.

Ennis J (2012) Swapping PINs for palms—The potential of biometric technology in retail banking. *Biometric Tech. Today* 4:8–9.

Esposito Vinzi V, Trinchera L, Amato S (2010) PLS path modeling: From foundations to recent developments and open issues for model assessment and improvement. Esposito Vinzi V, Chin WW, Henseler J, Wang H, eds. *Handbook of Partial Least Squares: Concepts, Methods and Applications* (Springer, Berlin Heidelberg), 47–82.

Falk RF, Miller NB (1992) *A Primer for Soft Modeling*, 1st ed. (University of Akron Press, Akron, OH).

Flavián C, Guinalíu M (2006) Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Indust. Management Data Systems* 106(5):601–620.

Flavián C, Guinalíu M, Torres E (2005) The influence of corporate image on consumer trust: A comparative analysis in traditional versus Internet banking. *Internet Res.* 15(4):447–470.

Fornell C, Larcker DF (1981) Evaluating structural equation models with unobservable variables and measurement error. *J. Marketing Res.* 18(1):39–50.

Frewer L, Lassen J, Kettlitz B, Scholdered J, Beekman V, Berdal KG (2004) Societal aspects of genetically modified foods. *Food Chemical Toxicology* 42:1181–1193.

Gefen D, Straub DW (2005) A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Comm. Assoc. Inform. Systems* 16:91–109.

Gefen D, Karahanna E, Straub DW (2003) Trust and TAM in online shopping: An integrated model. *MIS Quart.* 27(1):51–90.

Gomez LM, Egan DE, Bowers C (1986) Learning to use a text editor: Some learner characteristics that predict success. *Human Comput. Interaction* 2:1–23.

Hassanein K, Head M (2007) Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *Internat. J. Human-Comput. Stud.* 65:689–708.

Herie M, Martin G (2002) Knowledge diffusion in social work: A new approach to bridging the gap. *Soc. Work* 47(1):85–95.

Hong W, Chan FK, Thong JY, Chasalow LC, Dhillon G (2014) A framework and guidelines for context-specific theorizing in information systems research. *Inform. Systems Res.* 25(1):111–136.

Hossain MA (2014) Exploring the perceived measures of privacy: RFID in public applications. *Australasian J. Inform. Systems* 18(2): 133–148.

Hossain MA, Dwivedi YK (2014) What improves citizens' privacy perceptions toward RFID technology? A cross-country investigation using mixed method approach. *Internat. J. Inform. Management* 34(6):711–719.

Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. *IEEE Trans. Circuits Systems Video Tech.* 14(1):14–20.

James T, Pirim T, Boswell K, Reithel B, Barkhi R (2006) Determining the intention to use biometric devices: An application and

extension of the technology acceptance model. *J. Organ. End User Comput.* 18(3):1–24.
Johns G (2006) The essential impact of context on organizational behavior. *Acad. Management Rev.* 31(2):386–408.
Jones LA, Ant AI, Earp JB (2007) Towards understanding user perceptions of authentication technologies. Yu T, ed. *Proc. 2007 ACM Workshop Privacy Electronic Soc.* (ACM, New York), 91–98.
Keppel G (1991) *Design and Analysis: A Researcher's Handbook* (Prentice-Hall, Englewood Cliffs, NJ).
Kulviwat S, Bruner GC, Kumar A, Nasco SA, Clark T (2007) Toward a unified theory of consumer acceptance technology. *Psych. Marketing* 24(12):1059–1084.
Landis JR, Koch GG (1977) The measurement of observer agreement for categorical data. *Biometrics* 33(1):159–174.
Lee AS, Baskerville RL (2003) Generalizing generalizability in information systems research. *Inform. Systems Res.* 14(3):221–243.
Liang H, Xue Y (2009) Avoidance of information technology threats: A theoretical perspective. *MIS Quart.* 33(1):71–90.
Majchrzak A, Cotton J (1988) A longitudinal study of adjustment to technological change: From mass to computer-automated batch production. *J. Occupational Psych.* 61:43–66.
Meyers LS, Gamst G, Guarino AJ (2006) *Applied Multivariate Research: Design and Interpretation* (Sage Publications, Thousand Oaks, CA).
Mick DG, Fournier S (1998) Paradoxes of technology: Consumer cognizance emotions, and coping strategies. *J. Consumer Res.* 25: 123–143.
Miltgen CL, Popovic A, Oliveira T (2013) Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decision Support Systems* 56: 103–114.
Morosan C (2011) Customers' adoption of biometric systems in restaurants: An extension of the technology acceptance model. *J. Hospitality Marketing Management* 20:661–690.
Morosan C (2012a) Understanding the antecedents of perceived value of registered traveler biometric systems. *J. Hospitality Marketing Management* 21:872–896.
Morosan C (2012b) Voluntary steps toward air travel security: An examination of travelers' attitudes and intentions to use biometric systems. *J. Travel Res.* 51(4):436–450.
Morosan C (2012c) Theoretical and empirical considerations for guests' perceptions of biometric systems in hotels: Extending the technology acceptance model. *J. Hospitality Tourism Res.* 36(52): 52–84.
Norman P, Searle A, Harrad R, Vedhara K (2003) Predicting adherence to eye patching in children with amblyopia: An application of protection motivation theory. *British J. Health Psych.* 8(1): 67–82.
Oliver RL (1980) A cognitive model of the antecedents and consequences of satisfaction decisions. *J. Marketing Res.* 17(4):460–469.
Orlikowski W, Iacono C (2001) Research commentary: Desperately seeking the "IT" in IT research: A call to theorizing the IT artifact. *Inform. Systems Res.* 12(2):121–134.
Patil HK, Seshadri R (2014) Big data security and privacy issues in healthcare. Chen P, Jain H, eds. *Proc. 2014 IEEE Internat. Congress Big Data* (IEEE Computer Society, Los Alamitos, CA), 762–765.
Patil P, Palwe R, Kulkarni G, Belsare S, Koli K (2015) Cloud security issues. *J. Inform. Engrg. Appl.* 5(1):31–34.
Pavlou PA, Liang H, Xue Y (2007) Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quart.* 31(1):105–136.
Peter JP, Tarpey LX Sr (1975) A comparative analysis of three consumer decision strategies. *J. Consumer Res.* 2(1):29–37.
Prabhakar S, Pankatani S, Jain A (2003) Biometric recognition: Security and privacy concerns. *IEEE Security Privacy* 1(2):33–42.
Ringle CM, Wende S, Will A (2005) SmartPLS 3.2.0. SmartPLS, Hamburg, Germany.
Rogers EM (2003) Elements of diffusion. *Diffusion Innovations* 5:1–38.
Rogers RW (1975) A protection motivation theory of fear appeals and attitude change. *J. Psych.* 91:93–114.
Rousseau DM, Fried Y (2001) Location, location, location: Contextualizing organizational research. *J. Organ. Behav.* 22:1–13.
Sakharova I (2012) Payment card fraud: Challenges and solutions. Zeng D, Zhou L, Cukic B, Wang GA, Yang CC, eds. *IEEE Internat. Conf. Intelligence Security Informatics* (IEEE, Piscataway, NJ), 227–234.
Schwartz SH (1992) Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. *Experimental Social Psychology* (Academic Press, San Diego).
Sheng H, Nah FF, Siau K (2008) An experimental study on U-commerce adoption: Impact of personalization and privacy concerns. *J. Assoc. Inform. Systems* 9(6):344–376.
Smith HJ, Dinev T, Xu H (2011) Information privacy research: An interdisciplinary review. *MIS Quart.* 35(4):989–1016.
Straub D, Boudreau MC, Gefen D (2004) Validation guidelines for IS positivist research. *Comm. Assoc. Inform. Systems* 13(24):380–427.
Straub DW (1989) Validating instruments in MIS research. *MIS Quart.* 13(2):147–169.
Straub ET (2009) Understanding technology adoption: Theory and future directions for informal learning. *Rev. Educational Res.* 79(2):625–649.
Strauss AL, Corbin J (1990) *Basics of Qualitative Research* (Sage, London).
Tene O, Polonetsky J (2012) Privacy in the age of big data: A time for big decisions. *Stanford Law Rev. Online* 64:63–69.
Tenenhaus M, Vinzi VE, Chatelin YM, Lauro C (2005) PLS path modeling. *Computational Statist. Data Anal.* 48:159–205.
Teo HH, Oh LB, Liu C, Wei KK (2003) An empirical study of the effects of interactivity on web user attitude. *Internat. J. Human-Comput. Stud.* 58(3):281–305.
Thomsen CJ, Borgida E, Lavine H (1995) The causes and consequences of personal involvement. Petty RE, Krosnick JA, eds. *Attitude Strength: Antecedents and Consequences* (Lawrence Erlbaum, Hillsdale, NJ), 191–214.
Venkatesh V, Bala H (2008) Technology acceptance model 3 and a research agenda on interventions. *Decision Sci.* 39(2):273–315.
Venkatesh V, Thong JY, Xu X (2016) Unified theory of acceptance and use of technology: A synthesis and the road ahead. *J. Assoc. Inform. Systems* 17(5):328–376.
Wagner N, Hassanein K, Head M (2010) Computer use by older adults: A multidisciplinary review. *Comput. Human Behav.* 26(5): 870–882.
Whetten DA (2009) An examination of the interface between context and theory applied to the study of Chinese organizations. *Management Organ. Rev.* 5(1):29–55.
Xu H (2007) The effects of self-construal and perceived control on privacy concerns. Rivard S, Webster J, eds. *Proc. Twenty Eighth Internat. Conf. Inform. Systems* (Curran Associates, Red Hook, NY), 1–14.
Xu H, Dinev T, Smith J, Hart P (2011) Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *J. Assoc. Inform. Systems* 12(12):798–824.
Yoon C, Rolland E (2012) Knowledge-sharing in virtual communities: Familiarity, anonymity and self-determination theory. *Behav. Inform. Tech.* 31(11):1133–1143.
Yousafzai SY, Pallister JG, Foxall GR (2003) A proposed model of e-trust for electronic banking. *Technovation* 23:847–860.