5-2019

THE FUTURE OF IDENTITY MANAGEMENT: UNDERSTANDING CONSUMER ATTITUDES TOWARDS BIOMETRIC IDENTIFICATION

Annette M. Mills
University of Canterbury, annette.mills@cantebury.ac.nz

Zhanhong Zheng
University of Canterbury, zzh119@uclive.ac.nz

THE FUTURE OF IDENTITY MANAGEMENT: UNDERSTANDING CONSUMER ATTITUDES TOWARDS BIOMETRIC IDENTIFICATION

Annette M. Mills
University of Canterbury
annette.mills@cantebury.ac.nz

Zhanhong Zheng
University of Canterbury
zzh119@uclive.ac.nz

Abstract

The explosive growth of consumer-facing biometric technology is providing opportunities for organizations to change the way in which they identify and authenticate consumers, and replace traditional forms of identification such as usernames and passwords. For consumers, the benefits include increased account security and convenient access to services. However, these positives can be countered by issues such as concerns about privacy and security. Drawing on Protection Motivation Theory (PMT) and prior research, this study uses data collected from 132 online banking consumers to assess the relative impacts of benefits and concerns on their attitude towards using biometric identification for their banking. Implications for practice and future research are discussed.

Keywords

Biometric identification, Protection Motivation Theory, Attitude, Privacy, Security, Online Banking,

THE FUTURE OF IDENTITY MANAGEMENT: UNDERSTANDING CONSUMER ATTITUDES TOWARDS BIOMETRIC IDENTIFICATION

1. Introduction

Biometric identification refers to the use of people's unique physiological and behavioural characteristics to verify their identity and authenticate their access to a service, account or digital device. The aim is to recognise an individual automatically by assessing user-provided characteristics, which are not able to be shared or copied by others and comparing this with previously collected information (Ogbanufe & Kim, 2018). The most common systems use fingerprints, voice recognition, and facial recognition.

Biometric technologies have been in existence for decades, being mostly used by governments, the military and on a large scale in airports for immigration clearance. With the explosive growth of consumer-facing biometric technology there has been a surge in interest in its application in the business environment. While benefits such as convenience and increased security may attract consumers, beyond its use to unlock devices such as mobile phones, tablets and computers, consumers have been reluctant to use biometric identification on a large scale (German & Barber, 2018). Indeed studies show an unease towards biometric technologies particularly in relation to privacy, security, and vulnerability to identity theft (German & Barber, 2018; Kessem, 2018). These concerns could undermine the wide scale uptake of the technology, despite its benefits. Understanding both the benefits and concerns that people perceive in relation to biometric identification and the relative impacts requires continuous investigation to better inform practice and research of what needs to be addressed in the wake of a rapidly changing landscape of individual identification.

2. Prior Research and Model Development

The last decades have been dominated by the increasing need for and use of tokens and passwords to secure access to various devices and services such as mobile phones and online accounts. However, this combination of usernames, passwords and PINs are not always adequate for digitally identifying and authenticating people and, avoiding data breaches and other losses. As the technology matures and people become more comfortable with it, many organisations are starting to use biometrics (e.g. face, fingerprint and voice recognition) as a way to verify and authenticate individuals.

At the same time, although biometric identification in the consumer marketplace is increasing, its use does raise issues related to security and privacy. For example, in a recent study of consumer attitudes towards biometric authentication, German and Barber (2018) found that while 42% of consumer used biometrics to unlock their devices, only 17% used it for personal banking. For those who were not comfortable with using biometrics, privacy invasion and identity theft were among the most cited reasons for their discomfort. In another study on the Future of Identity (Kessem, 2018) it was reported that while 87% of respondents would consider using biometric authentication in the future, when it comes to the 'most trusted', more than half did not trust financial institutions to protect their biometrics information, and only 15% trusted social media sites. So despite its popularity, the study showed that concerns about privacy and security persist, with 25% of the respondents not trusting any organisation to protect their biometric data (Kessem, 2018). This is consistent with earlier studies, which also suggest that reluctance to use biometrics is due to reasons such as concerns that biometric data may be permanently compromised if the data were stolen, beliefs that the technologies still need to be improved and privacy concerns (Breward et al., 2017; Rawlson, 2015).

The idea of using biometrics to identify and authenticate individuals is not new. Indeed researchers have been investigating its potentials for decades. But it is only within the last several years that the technology has matured enough to now become a feature of consumer-held devices making it viable option for businesses to adopt on a wide scale. But to be successful, people need to be willing to use it. To understand people's attitude towards and willingness to use biometric identification, prior research has used theories such as the Technology Acceptance Model (TAM), the Theory of Reasoned Action (TRA), the Unified Theory of Acceptance and Use of Technology (UTAUT) and Protection Motivation Theory (PMT) (Miltgen, et al., 2013; Ngugi & Kamis, 2013; Seyal & Turner, 2013). These show that factors such as perceived usefulness, compatibility, facilitating conditions, perceived risks, trust in technology, self-efficacy, privacy invasion, response efficacy, attitude and subjective norms impact biometric use (Miltgen et al., 2013; Ngugi & Kamis, 2013; Seyal & Turner, 2013). A few have also examined biometric identification applications in the banking sector (Breward et al., 2017; Ngugi & Kamis, 2013; Ogbanufe & Kim, 2018) giving insights in to contextual factors that impact user acceptance. These suggest that privacy and security are the main concerns inhibiting uptake, while convenience and account security motivate use.

Drawing on aspects of Protection Motivation Theory (PMT) in combination with prior research on security and privacy concerns (Jansen & van Schaik, 2018; Johnston & Warkentin, 2010; Ngugi & Kamis, 2013; Rogers, 1975) this study proposes a model of biometric acceptance that aims to extend current understanding of the risks and benefits trade-offs that impact people's attitudes regarding biometric identification. Although prior research has examined similar concepts, as the technology matures and becomes an increasingly viable option for consumer authentication, it is timely to determine whether and to what extent do concerns about security and privacy continue to frame people's views about biometric identification. In this study, we will examine people's views of biometric identification in one of the most trusted of contexts – banking, focusing on persons who do not use biometric identification for online banking.

2.1 The Research Model

Based on expectancy-value theory, Protection Motivation Theory (PMT) which was developed in the health field was aimed at demonstrating how fear appeals can impact peoples' attitude and behaviour (Rogers, 1975). Though the initial focus of the PMT was on fear appeals, the model has been successfully used to examine decision-making related to risk (Maddux & Rogers, 1983), as well as prevention and precautionary behaviours (Floyd, Prentice-Dunn & Rogers, 2000; Jansen & van Schaik, 2018; Johnston & Warkentin, 2010). The PMT comprises two key appraisals in determining motivation to take protective actions: (i) the threat appraisal which considers the risk associated with not taking action, and (ii) the coping appraisal which looks at ones' ability to reduce and even eliminate identified threats; this includes consideration of the costs and risks associated with taking the protective action. In this study the focus is on the *coping appraisal* (Rippetoe & Rogers, 1987) that is one's evaluation of the benefits and the risks associated with using biometric identification.

Prior research suggests the most salient factors impacting biometric identification acceptance are concerns about privacy and security and, benefits such as account security and user convenience (Breward, et al., 2017; Ogbanufe & Kim, 2018). Although these are collectively part of the coping appraisal, risks and concerns act in opposition to benefits. If sufficiently strong, these concerns would discourage people from using biometrics. As such this study will look at the impacts of privacy concerns, security concerns, and perceived vulnerability to biometric information being compromised and, key benefits of account security and convenience, on attitude towards biometrics. See Figure 1.

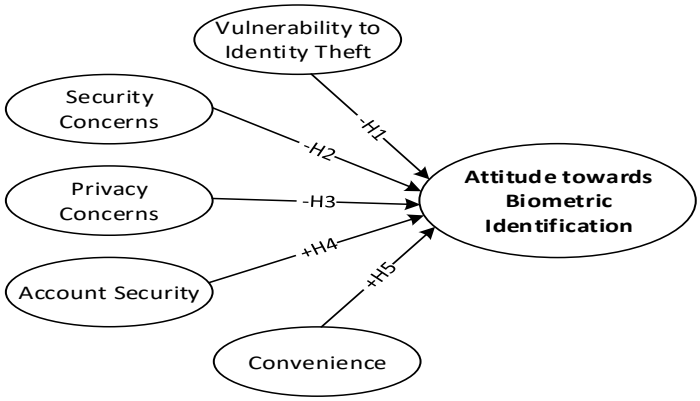

Fig 1: The Research Model

2.2. Hypothesis Development

Perceived vulnerability refers to people's assessment of the possibility that they will be threatened by adverse events (Boss et al., 2013; Johnston & Warkentin, 2010; Rogers, 1975). Although this construct is most often examined as part of the threat appraisal and as a motivator to take protective actions such as following safety guidelines to mitigate online banking fraud (Jansen & van Schaik, 2018), it has also been conceptualised as an inhibitor and therefore as part of the coping appraisal, wherein people may find themselves threatened by an adverse event should they take the protective action (Ngugi & Kamis, 2013). In this case, people may believe that use of their biometric information increases their vulnerability to identity theft and their information being compromised. Prior research, though limited, has suggested that perceived vulnerability can impact people's attitudes such that they avoid using a novel technology (Ngugi & Kamis, 2013; Rippetoe & Rogers, 1987). Thus, if persons believe that using biometric identification for online banking raises their vulnerability to adverse events such as identity theft and their information being compromised, they are less likely to favour its use. Hence:

H1: Perceived vulnerability is inversely related to attitude towards using biometric identification

Privacy concern reflects an individuals' concerns about organisational practices that may result in a possible loss of privacy – these include concerns about data collection, unauthorised secondary use, improper access and errors (Smith et al., 1996). Where such concerns are elevated, they have been shown to negatively impact people's willingness to use biometric identification (Breward, et al., 2017). Arguably, this may be because people see the technology as privacy invading, with recent surveys showing that people are most concerned about how their biometric data are used and potential misuse (German & Barber, 2018; Kessem, 2018). So although, major financial institutions, when compared to social media and online retailers, are the more trusted to keep biometric data safe (Kessem, 2018), privacy concerns may still impact use of biometric identification. Hence it is expected that:

H2: Privacy concern is inversely related to attitude towards using biometric identification

The use of biometric identification in online banking means that, with the current technologies, users' unique biometric data must be collected and held by the service provider. In this context, *security concern* reflects consumers' beliefs that the service provider may not be able to adequately protect their biometric information from being accessed and manipulated by unauthorised parties (Flavián & Guinalíu, 2006). As such, if banking consumers have concerns about the protection of their biometric identification, this may negatively impact their attitude towards its use (Breward, et al., 2017). Hence it is proposed:

H3: Security concern is negatively related to attitude towards using biometric identification

Next, we consider benefits of biometric identification, i.e. account security and convenience.

Perceived account security indicates consumers' beliefs that biometric identification can help protect and avoid unauthorised access to their accounts (Breward, et al., 2017). In the case of online banking, traditional ways of identification, such as using a bank card and Personal Identification Number (PIN) to access bank accounts can lead to problems including card fraud, personal accounts being accessed by unauthorised parties and the interception of financial data (Sakharova, 2012). These concerns, coupled with the facts that biometrics re not easily lost or forgotten and are difficult to forge (Jain et al., 2004), are encouraging banks to use biometrics as a way of authenticating customers and protecting their accounts. This increased security may also encourage individuals to evaluate biometric identification favourably (Breward, et al., 2017; Ogbanufe & Kim, 2018). Hence it is expected that:

H4: Account security is positively related to attitude towards using biometric identification

Convenience relates to consumers' beliefs that using biometric identification provides quick and easy access to devices and accounts (Breward, et al. 2017). In the case of online banking, given that consumers should change passwords regularly and not use similar passwords across multiple accounts, utilising bank cards and PINs can require consumers to remember several passwords. Biometric identification on the other hand can significantly enhance user convenience as they are "no longer required to remember multiple, long and complex frequently changing passwords" (Jain et al., 2004, p12). Biometrics also often enables quicker access to devices and accounts and is more easily operated (Ogbanufe & Kim, 2017). Hence:

H5: Convenience is positively related to attitude towards using biometric identification

3. Methodology and Results

Banks and other organisations worldwide are trialling various applications and technologies to support biometric identification. The most common is fingerprint recognition followed by voice and facial recognition. In New Zealand, these technologies are being rolled out in the financial sector; thus New Zealand is considered a suitable context to assess people's perceptions about biometrics. To assess the research model, survey data was collected from 132 online banking customers who do not use biometric identification for online banking. 45.5% were female and 55.5% male; 49 (37.1%) were aged 18-29 years, 62 (47%) aged 30-49 years, and the remaining 21 (15.9%) aged 50 years and over.

All constructs were adapted from existing sources: privacy concern (3 items), security concern (3 items), convenience (3 items), account security (2 items), perceived vulnerability (2 items), and attitude (3 items) (Ajzen & Fishbein 1980; Breward, et al., 2017; Johnston & Warkentin, 2010). Responses were on 7-point Likert scales with Strongly Disagree and Strongly Agree as end-points. Sample items are in Appendix 1.

3.1 Data Analysis and Results

The research model was assessed using the Partial Least Squares (PLS) approach to structural equation modelling and the bootstrapping procedure with 500 resamples (Chin, 2010). SmartPLS 3.2.7 was used.

All constructs except privacy concerns were modelled as reflective. For these constructs, the results showed most item loadings exceeded the suggested threshold of 0.707 ranging from 0.716 to 0.845, except for one item measuring account security with a factor loading of 0.682 and just below the recommended threshold of 0.707 (Chin 2010). Composite reliability values

ranged from 0.727 to 0.849 (except for account security at 0.657) and average variance extracted (AVE) from 0.571 to 0.652, except for account security (0.489). All constructs, except for account security (which was just below recommended thresholds), exceeded recommended cut-offs of 0.707 and 0.50 for composite reliability and AVE, respectively suggesting adequate convergence of the measures (Chin 2010). The results also showed construct AVEs were greater than the squared correlations among the constructs, and at the item level that all loadings exceeded the cross-loadings. Altogether these results suggest adequate discriminant validity for the measures at the construct and item levels (Chin 2010).

Privacy concern was modelled as formative. Item loadings showed two items related to the collection and to the secondary use of personal data were significant (at 0.492 and -0.602 respectively) as well as the weights (at 0.856 and -0.952, respectively).

For the structural model, the results explained 0.422 of the variance observed for attitude towards biometric identification. Convenience (β=0.532; $p \leq 0.001$) was the strongest variable followed by account security (β=0.172; $p \leq 0.10$) and security concerns (β= -0.116; $p \leq 0.10$), supporting H2, H4 and H5 respectively. However, perceived vulnerability (β=0.034) and privacy concern (0.096) were not significant; H1 and H3 were not supported.

4. Discussion and Conclusion

With the surge in consumer-facing biometric technologies, biometric identification is poised to play an increasing role in consumer services such as online banking. However, their success will depend on wide scale consumer acceptance and uptake. Yet, studies show that even though many are using biometrics and people are amendable to using some form of biometrics in the future (Kessem, 2018) there are concerns, with less than half not trusting that institutions will adequately protect their biometric information. Focusing on those who do not use biometric identification for online banking, this study examined consumer perceptions of the benefits of biometrics (i.e. increased convenience and account security) and the counter negative influences of privacy concerns, security concerns and vulnerability to one's biometric identity being compromised on people's attitude towards biometric identification, looking at one of the most 'trusted' of sectors - banking services (Kessem, 2018).

The results showed that user convenience and account security were the most significant determinants, exerting a positive impact on attitude towards biometric identification while security concerns had a negative influence on attitude. Consistent with prior research, these results suggest that people are likely to trade-off their security concerns for increased user convenience and account security (Breward et al., 2017; Kessem, 2018), provided there are enough security measures in place to protect their biometric information. The results further suggest some softening in consumer views in relation to privacy concerns which in contrast to prior research (Breward et al., 2017; Ngugi & Kamis, 2013), did not have a significant impact on consumer attitude. Vulnerability to the compromise of one's biometric identity was also not significant; this suggests that although consumers had general concerns about the security of their biometric information, they did not seem to believe they were at risk of their information being compromised. This outcome may be due to increased user awareness of and comfort with using biometric identification (e.g. to unlock devices), and technology improvements that make it difficult to forge one's biometric identity (e.g. with online biometrics-based recognition systems require the person to be recognized to be present at the point (Jain et al. 2004)). It may also be that this type of threat is not being widely felt in New Zealand, whereas for other countries such as the USA where there have been reports of significant losses of people's biometric information (e.g. fingerprints) (German & Barber,

2018; Kremling & Parker, 2018) privacy concerns and concerns about identity theft may be elevated and more impactful on attitudes.

Taken together, the findings of this study have important implications for practice. They demonstrate that as organisations begin to rollout biometric technologies they need to provide assurances to consumers around the safety of their biometric data. Given the importance of convenience, it is important too that the services are easy to use, and inconveniences such as the need to re-verify one's biometrics is minimised. Finally, although the results did not show that privacy concerns or vulnerability to one's identity being compromised impact attitude, should these become problematic the impacts could be significant and should not be ignored in the design of new systems.

For this study, there are limitations and opportunities for future research. For example, there are other factors such as threat severity, self-efficacy and trust that could be included to more comprehensively assess peoples' attitudes (Boss, et al, 2015; Jansen & van Schaik, 2018). The research also only surveyed persons in New Zealand, where use of biometrics is optional; only persons who do not use biometric identification for banking were surveyed. These results contrast studies set in other contexts and countries such as the USA which showed that privacy and security concerns have stronger and negative effects (Breward et al., 2017; Ngugi & Kamis, 2013; Ogbanufe & Kim, 2018) when compared with benefits such as increased user convenience. These findings signal the importance of considering the context in which new and emerging technologies are evaluated, and the need for future work to contextualise the study of biometrics identification and its use.

References

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

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, 39(4), 837-864

Breward, M., Hassanein, K., & Head, M. (2017). Understanding Consumers' Attitudes toward Controversial Information Technologies: A Contextualization Approach. *Information Systems Research*, 28(4), 760-774.

Chin W.W. (2010). How to Write Up and Report PLS Analyses. In: Esposito Vinzi V., Chin W., Henseler J., Wang H. (eds), *Handbook of Partial Least Squares*. Springer Handbooks of Computational Statistics. Springer, Berlin, Heidelberg, 655-690.

Flavián, C., & Guinalíu, M. (2006). Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web Site. *Industrial Management & Data Systems*, 106(5), 601-620.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, 30(2), 407-429.

German, R. L. and Barber K. S. (2018). Consumer Attitudes about Biometric Authentication: A UT CID Report, Retrieved from https://identity.utexas.edu/assets/uploads/publications/Consumer-Attitudes-About-Biometrics.pdf

Kessem, L. (2018). IBM Security: Future of Identity Study, Retrieved from https://www.ibm.com/security/data-breach/identity-report-user-study

Kremling, J. & Sharp Parker, A.M. (2018). Cyberspace, Cybersecurity, and Cybercrime, SAGE Publications.

Jansen, J., & van Schaik, P. (2018). Testing a Model of Precautionary Online Behaviour: The Case of Online Banking. *Computers in Human Behavior*, 87(October), 371-383

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3), 549-566.

Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation and Self-efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology*, 19(5), 469-479.

Miltgen, C., Popovič, 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(1), 103-114.

Ngugi, B., & Kamis, A. (2013). Modeling the Impact of Biometric Security on Millennials' Protection Motivation. *Journal of Organizational and End User Computing*, 25(4), 27-49.

Ogbanufe, O., & Kim, D. J. (2018). Comparing Fingerprint-based Biometrics Authentication versus Traditional Authentication Methods for e-Payment. *Decision Support Systems*, 106, 1-14.

Rawlson, O. (2014, November) Banking and Biometrics White Paper. Retrieved from https://www.biometricupdate.com/wp-content/uploads/2014/12/Biometrics-and-Banking-Special-Report-2014.pdf

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of Components of Protection-Motivation theory on Adaptive and Maladaptive Coping with a Health Threat. *Journal of personality and social psychology*, 52(3), 596-604.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology*, 91(1), 93-114.

Sakharova, I. (2012). Payment Card Fraud: Challenges and Solutions. *Proceedings: IEEE International Conference on Intelligence and Security Informatics*, 11-14 June, Arlington, VA, 227-234.

Seyal, A. H., & Turner, R. (2013). A Study of Executives' Use of Biometrics: An Application of Theory of Planned Behaviour. *Behaviour & Information Technology*, 32(12), 1242-1256.

Appendix 1: Sample Items

Constructs	Items
Perceived Vulnerability	I would be at risk of my biometric identification information being compromised, if I use it for online banking.
Privacy Concern	It would bother me if my bank asks me for biometric identification.
Security Concern	I would not feel totally safe providing my biometric information to my bank.
Account Security	Using biometric identification for online banking would reduce the risk of my bank account being compromised.
Convenience	Using biometric identification for online banking would enable me to do my banking more quickly.
Attitude	Using biometric identification for online banking is a good idea.