WCET#1811184, VOL 0, ISS 0

Biometric technologies at music festivals: An extended technology acceptance model

Lauren Norfolk and Michael O'Regan

QUERY SHEET

This page lists questions we have about your paper. The numbers displayed at left are hyperlinked to the location of the query in your paper.

The title and author names are listed on this sheet as they will be published, both on your paper and on the Table of Contents. Please review and ensure the information is correct and advise us if any changes need to be made. In addition, please review your paper as a whole for typographical and essential corrections.

Your PDF proof has been enabled so that you can comment on the proof directly using Adobe Acrobat. For further information on marking corrections using Acrobat, please visit http://journalauthors.tandf.co.uk/production/acrobat.asp; https://authorservices.taylorandfrancis.com/how-to-correct-proofs-with-adobe/

The CrossRef database (www.crossref.org/) has been used to validate the references.

AUTHOR QUERIES

Q1 Please provide the missing department name for the author's affiliation and correspondence footnote.

Q2 The corresponding author details have been imported from data supplied with the original manuscript. Please revise if incorrect.

Q3 The keywords section has been imported from data supplied with the original manuscript. Please revise if incorrect.

Q4 Please provide complete details for (Perala, 2018, Davis, Bagozzi, & Warshaw, 1989a, Saade and Bahli 2005, Giesing, 2003, Sun, 2003, Wilkinson 2016, and Vijayasarathy 2004) in the reference list or delete the citation from the text.

Q5 Please provide the missing conference location in all conferences and proceedings references.

Q6 There is no mention of (Davis 1985, Liu et al. 2010, and Schreiber-Gregory 2018) in the text. Please insert a citation in the text or delete the reference as appropriate.

Q7 Please provide the page range.

JOURNAL OF CONVENTION & EVENT TOURISM
https://doi.org/10.1080/15470148.2020.1811184

Routledge
Taylor & Francis Group

Biometric technologies at music festivals: An extended technology acceptance model

Lauren Norfolk and Michael O'Regan

Q1 Bournemouth University, Poole, Dorset, UK

ABSTRACT

The purpose of this paper is to gain a better understanding of user acceptance of Biometric Technologies (BT) at outdoor music festivals in the United Kingdom. While research on such technologies, such as facial recognition is limited in the events context, they have already been deployed at music festivals to deal with issues of security, safety and crowd management. Using an extended Technology Acceptance Model (TAM), a self-administered questionnaire was completed by young Q3 adults in the United Kingdom who had previously been to a music festival. The study found factors such as privacy, reliability and accuracy did not have a significant impact on user acceptance. Other factors, such as trust, compatibility and convenience were found to have a significant positive impact on perceived ease of use, perceived usefulness and attitude to use. As the findings indicate that accuracy and privacy do not impact BT acceptance, the paper explores how organizers can be transparent and accountable as to their intentions to use BT, so as to justify the usefulness of BT to attendees, artists, regulators and authorities.

ARTICLE HISTORY
Received 29 January 2020
Revised 7 July 2020
Accepted 8 July 2020

KEYWORDS
Biometric technologies; event management; facial recognition; music festivals; technology acceptance model

Introduction

There were 700 music festivals, attended by 7.1 million customers in the United Kingdom (UK) during 2018 (CGA, 2019). The sector is worth US$3.25 billion annually in the UK, and the primary consumers are aged beween 16-19 years (49%) and between 20-39 years (43%) (Mintel, 2019). However, issues related to perceived risk, security and safety at festivals have emerged, with Mintel (2017) finding that 44% of attendees feel unsafe at music festivals; with 58% of males aged 16-34 years, more likely to feel unsafe, as opposed to 53% of women in the same age group. Whilst recent media and scholarly research have focused on racism, homophobia, transphobia, xenophobia and sexual harassment at festivals (Davies, 2017; Gisbert & Rius-Ulldemolins, 2019), Mintel (2017) found violence and drugs as the primary perceived risk factors. Other issues are related to fraud, theft

CONTACT Michael O'Regan moregan@bournemouthac.uk Bournemouth University, Fern Barrow, Talbot Q2 Campus, Poole, Dorset BH12 5BB, UK.

and criminality (Aviva, 2012) and the threat of terrorism (Millward, 2016). Bowdin, Allen, Harris, McDonnell, and O'Toole (2012) argue that events are particularly susceptible to risks, given the movement of attendees, staff, volunteers, and equipment. In response, festivals have sought to embed measures to make attendees feel safe and secure. This has often led to greater use of security. However, Boyle and Haggerty (2012, p. 255) argue that the "emphasis on raising the visibility of security may also serve to amplify rather than dampen uncertainty." This has driven the broader events sector to look at new systems of identification and verification that reduces perceived risks and increases perceived security, without being intrusive. This has spurned new ideas within the sector, as to how to utilize biometric technologies (BT) for security and safety, as well as other processes, such as registration and payments. COVID-19 has also driven the sector to look for replacement systems to identify and verify individuals without the risk of close contact, with facial recognition companies such as Wisesoft (China) adapting their facial recognition systems to check temperatures.

Garg and Singh (2014, p. 296) define BT as "a pattern recognition system that recognizes a person by determining the authentication by using his different biological features." While a person can be identifiable through an identity card, a password or personal identification number (PIN), identity can also be based on something you are or have, such as a pattern of ridges on a fingertip (Davies, 1994). This form of identification is known as biometrics, with BT often framed as possibility changing the world, as it alters our experiences at airports, railway stations, schools, retail outlets, public spaces, and large events (Stikeman, 2003). They can, for example, be used at events, to speed up traffic and security checks, improve queue management through automated check-in/check-out processes, and therefore saving time for attendees and reducing congestion. However, there are conflicting reports as to the comfort rate amongst the general public and event attendees for particular BT, such as facial recognition, iris scanning, and fingerprinting (IBM Security, 2018). The acceptance of BT amongst festival goers is of key interest to BT companies, event organizers, police and security services, as well as local and national authorities. This study identifies and evaluates acceptance of BT systems at outdoor festivals in the UK, amongst 18-25 year old festival goers using the Technology Acceptance Model (TAM), before exploring the implications for the festival sector.

Biometric technologies (BT)

As identities "are the traits and characteristics, social relations, roles, and social group memberships that define who one is" (Oyserman, Elmore, &

Smith, 2012, p. 69), BT emerged to utilize those traits and characteristics for identification and verification purposes. As any "automatically measurable, robust and distinctive physical characteristic or personal trait" (Woodward, Horn, Gatune, & Thomas, 2003, p. 1) can be used to identify or verify an individual, the term *biometric* arose from the Greek words bios (life) and metrikos (measure) (Delac & Grgic, 2004). While BT identification and verification systems include vein infrared thermograms, gait, hand and finger geometry, keystroke dynamics, palm print, retina scanning, signature and voice tracts (Jain, Ross, & Prabhakar, 2004), the most commonly used BT systems involve facial recognition, iris scanning and fingerprinting. As facial recognition records the spatial geometry of unique features of the face (Bhatia, 2013), facial recognition systems, using cameras, can now identify a person from a distance (Hamid, 2015; Meng, Wong, Furnell, & Zhou, 2015; Woodward et al., 2003). Facial recognition systems are used to identify card counters in casinos, shoplifters in stores, criminals in urban areas and passengers in airports. Facial recognition is a BT accepted by many, given it is non-intrusive (Meng et al., 2015). While there are different types of facial recognition databases and algorithms (Patel & Yagnik, 2013), such as Amazon's Rekognition system, most facial recognition systems are used either in identification or verification mode (Jain et al., 2004). As new uses become apparent, it has been increasingly used in varied contexts. Airports and airlines are utilizing self-service facial recognition at check-in and at boarding gates, with the aim of improving speed and efficiency (Chan, 2017). Banks and payment providers utilize facial recognition on phones so as to reduce security breaches (Brathwaite, 2017). In China, authorities use facial recognition through next-generation Q4 CCTV and smart-glasses (Perala, 2018) in multiple contexts, from boarding a train, to checking into a hotel. There has been criticism of the accuracy of specific facial technology systems, as people's faces change over time with age, given weight changes, plastic surgery and cosmetic use (Buciu & Gacsadi, 2016; Hamid, 2015). Environmental conditions, such as light conditions, noise motion blur can also affect accuracy as well as the position and angle of the face (Buciu & Gacsadi, 2016). There is evidence to suggest that facial recognition systems are inaccurate in identifying women and people of color (Buolamwini & Gebru, 2018). While police use of facial recognition is accepted by British Courts, there has also been resistance by those who see facial recognition as inappropriate for legal, cultural and religious reasons (Lawson, 2003).

BT utilizing iris scanning, which measures the unique pattern in the colored part of the eye (Miltgen, Popovič, & Oliveira, 2013) are the most reliable BT, given each iris has approximately 266 unique characteristics, which are thought to remain stable over time (Cavoukian, 1999; Chowhan

& Shinde, 2008; Miltgen et al., 2013). However, there are some negative feelings toward iris scanning, as it needs to be done at close physical distance to the individual, and administered by a person if the technology is mobile. Accuracy can be impacted, if the iris is partially hidden by eyelids, eyelashes, lenses and reflections (Chowhan & Shinde, 2008). The third major BT, after facial recognition and iris scanning is fingerprint recognition, which is a well-known and understood form of identification, and has a reliable reputation for accuracy (Ho, Stephens, & Jamieson, 2003). Woodward et al. (2003) describe it as a digital version of the old ink and paper method. While fingerprinting had been the longest serving, most successful and popular method for identifying individuals (Jain & Kumar, 2012), new fingerprint scanners are primarily based on optical, capacitive, and ultrasonic sensors. From terminals at airport entry points to laptops, mobile phones, and personal digital handheld tablets (Ogbanufe & Kim, 2018), such sensors have become highly accepted, well known and understood by users in many parts of the world (Ho et al., 2003). As each and every fingerprint is different (Jain & Kumar, 2012), the insecurity associated with pins and passwords are reduced. While accuracy, ease of use and installation are advantages, injuries such as burns and cuts can hinder results (Ho et al., 2003). As fingerprint scanners usually require people to touch the same surface, the potentially spread of COVID-19 through an unclean scanner has become to be seen as a drawback.

Overall, while iris scanning and fingerprinting are seen to be the most accurate (Buciu & Gacsadi, 2016; Chowhan & Shinde, 2008; Ho et al., 2003; Pons & Polak, 2008; Woodward et al., 2003), facial recognition has the advantage of being able to scan a person from a distance. Each technology, if used alone to identify or verify someone, has disadvantages, given there may be noisy sensor data, lack of distinctiveness of the biometric trait, unacceptable error rates and spoof attacks (Galbally, Marcel, & Fierrez, 2014; Jain, Nandakumar, & Ross, 2005). While the use of two or more biometric systems simultaneously can overcome some of accuracy and security weakness of using one system (Delac & Grgic, 2004, Taouche, Batouche, Berkane, & Taleb-Ahmed, 2014), few institutions or organizations have developed or deployed multimodal biometric systems.

Perceptions of biometric technology

While BT has become more increasingly embedded in consumer devices such as laptops and phones (Nandakumar, Nagar, & Jain, 2007), Morosan (2012b) notes a conflict in study findings for the acceptance of BT amongst intended users. While industry reports often focus on high public acceptance amongst intended users (Juniper Research, 2017), BT acceptance has been dominated by scholarly output from criminal studies (Prabhakar, Pankanti, & Jain, 2003; Weaver, 2006) and explorations of technical issues such as accuracy and concerns over false rejection rates (FRR), false acceptance rates (FAR) and failure to enroll rates (FTER) (Bharadwaj, Vatsa, & Singh, 2014; Clarke, Furnell, & Reynolds, 2002; Down & Sands, 2004). Within the leisure, tourism and events sectors, studies have noted the acceptance of BT in restaurants (Morosan, 2011) and hotels (Morosan, 2012b; Murphy & Rottet, 2009). However, no studies exist within the events sector, despite BT increasingly trialed at events. Facial recognition, for example, was used by the Police in the United Kingdom at the Download Festival in 2019, the Notting Hill Carnival in 2016 and 2017 and Remembrance Day events at the Cenotaph in 2017, to understand whether it could be used for large crowds. Before the COVID-19 pandemic, further deployments at sporting events and music festivals were under consideration. Given there were a total of 722 deaths at music festivals between 1999 and 2014, caused predominantly by trampling and illicit drug overdoses (Turris & Lund, 2017); there is some justification to use BT at events to potentially increase safety. The choice to trial BT at events also suggests a risk to public health, personal security or the possibility of terror attacks (Vulliamy, 2016; Wilkinson, 2016). As no national camera surveillance network exists outside China (Lui & Xiqing, 2017), BT providers and intermediaries' often trial their systems at events to improve BT systems (Hanumanthappa, LourdhuSuganthi, & Karthik, 2015). Complex event environments can test identification and verification speeds, reliability and accuracy, along with algorithms and BT databases. Events can also be used to build BT databases, and BT success at events might suggest that the technology could be used in other complex environments like airports or crowded city centers.

A number of companies, either through standalone commercial efforts or in partnership with authorities, have developed BT systems for, or in support of the event sector (Dai, 2018; Nilsson, 2018). While many of these efforts seek to identify, locate and arrest wanted criminals (Perala, 2017), companies like Zeus Biometrics (zenus-biometrics.com) use closed facial recognition databases, through existing registration platforms, for use in conferences, exhibitions, trade-shows, and festivals. BT offers possibilities for speeding up identification and verification at registration, the reduction of queues, identifying whether crowds are seated or standing, drowsiness or inebriation amongst attendees, audience emotions and the blacklisting of those with particular medical or criminal histories (e.g., a history of drug dealing) (Arbon, 2004; Kavanagh, Baral, Milanga, & Sugarman, 2019). Particular societies, ethnic and interest groups might be cautious of BT, given BT are still relatively new, with legal and ethical issues linked to all

BT systems. Trocchia and Ainscough (2006) argue that a primary concern is with the technologies themselves. Accuracy is an issue noted by many researchers as a primary concern (Langenderfer & Linnhoff, 2005), given the possibility of misidentification. Ho et al. (2003, p. 3) describes accuracy as "the ability to correctly match a biometric sample with its template." The accuracy of biometrics is largely dependent on the technology, with the accuracy of facial recognition considered medium, fingerprinting considered high, and iris scanning considered very high (Ho et al., 2003). Martin (2017) reported that thirty-five false matches were made and an erroneous arrest took place at the 2017 Notting Hill Carnival. Therefore, the accuracy of BT is still a concern, and has been identified as an important variable in the extant literature.

Another issue identified in the literature as important regarding acceptance is reliability; given that BT systems can be compromised because of sabotage, intrinsic failures or administration abuse (Jain, Nandakumar, & Nagar, 2008). Langenderfer and Linnhoff (2005) found that consumers are concerned that the technology could fail whilst using it, even if there was no criminal intent. Privacy was also found to be an issue in the literature, with Normalini and Ramayah (2017) arguing that governments can use BT to minimize internal and external threats. While they may do so to improve safety, certain religious and civil liberty groups believe BT could lead to a digital panopticon, with BT systems powered by artificial intelligence (Liu & Silverman, 2001). However, individuals may be willing to accept BT and less privacy if they know that its use can be exchanged for better security (Davis & Silver, 2004; Halevi, Kuppusamy, Caiazzo, & Memon, 2015). Research has found that consumers do not fully understand BT and the issues surrounding privacy and security risks (Huys, 2014; Miltgen et al., 2013). Compatibility with the (festival) context is also an important element to be explored and identified. Moore and Benbasat (1991, p. 195) state that compatibility is "the degree to which an innovation is perceived as being consistent with the existing values, needs, and past experiences of potential adopter." As compatibility is positively related to user adoption (Uzoka & Ndzinge, 2009), it would also affect the intention to implement BT. In the context of this study, this would suggest that if BT is compatible in the festival setting, it is more likely to be accepted by users. Other issues about BT include existential worries, including moral concerns and socio-cultural considerations (National Research Council & Whither Biometrics Committee, 2010). There is concern that young adults in particular, are being socialized into accepting of BT, with Trocchia and Ainscough (2006) noting that BT is criticized for setting a rather dark precedent by conditioning young adults to embrace the idea of big brother-style biometric tracking. Indeed, Bakir, Cable, Dencik, Hintz, and McStay

Table 1. Variables impacting upon user acceptance of BT.

Factor	Author and year
Trust	Ho et al. (2003); Giesing (2003); Hassanein and Head (2007); Tung et al. (2008); Ha and Stoel (2008); Ngugi et al. (2011); Morosan (2012a)
Convenience	Trocchia and Ainscough (2006); Yoon and Kim (2007); Hsu and Chang (2013)
Security	Ho et al. (2003); Trocchia and Ainscough (2006); Jain et al. (2008); Ngugi et al. (2011); Yoon and Steege (2013); Westdorp (2015)
Privacy	Liu & Silverman (2001); Ho et al. (2003); Giesing (2003); Vijayasarathy (2004); Jain et al. (2008); Morosan (2012a)
Reliability	Deane et al. (1995); Ho et al. (2003); Morosan (2012b); Fairhurst (1997)
Accuracy	Ho et al. (2003); Langenderfer and Linnhoff (2005); Ngugi et al. (2011); Sidharta, Priadana, & Affandi. (2016)
Compatibility	Moore and Benbasat (1991); Vijayasarathy (2004); Jain et al. (2008); Chen et al. (2009); Lane and Stagg (2014)

(2015) go as far as to argue, that security-orientated surveillance technologies were effective security tools that could disrupt human rights. The literature and the researcher's knowledge of the events sector indicate the factors that could impact upon user acceptance of BT (Table 1).

Methodology

The technology acceptance model

The determinants of Information Systems (IS) usage and acceptance have long been an issue for researchers, with the technology acceptance model (TAM) (Davis, 1989a, Davis, Bagozzi, & Warshaw, 1989b) becoming the most widely used model in exploring the determinants of technology usage. The TAM, adapted for IS, is itself an adaptation of the Theory of Reasoned Action (TRA) which originates from social psychology. The TRA suggests that a person's behavior is determined by their intention to perform the behavior and that this intention is a function of their attitude toward the behavior and subjective norms (Fishbein & Ajzen, 1975). While the TRA is used to predict individuals' decisions and is designed to explain "virtually any human behavior" (Ajzen & Fishbein, 1980, p. 4), the TAM uses TRA as a theoretical foundation to identify how perceived usefulness (PU) and perceived ease of use (PEOU) affect users' attitudes and intentions to use a system or technology, which in turn affects actual use of a technology (Davis, Bagozzi, & Warshaw, 1989a). Over the past three decades, the TAM has assumed a strong position as a means to model and explain the determinants of user acceptance of a broad spectrum of IS and end-user technologies.

Given rapid technological change across many societies, researchers have identified barriers to new technology acceptance (Wu & Wang, 2005). The TAM can explain the general determinants of acceptance that lead to explaining users' behavior, with extensive empirical TAM studies ranging from acceptance of Personal Digital Assistants (PDAs) by physicians (Dee,

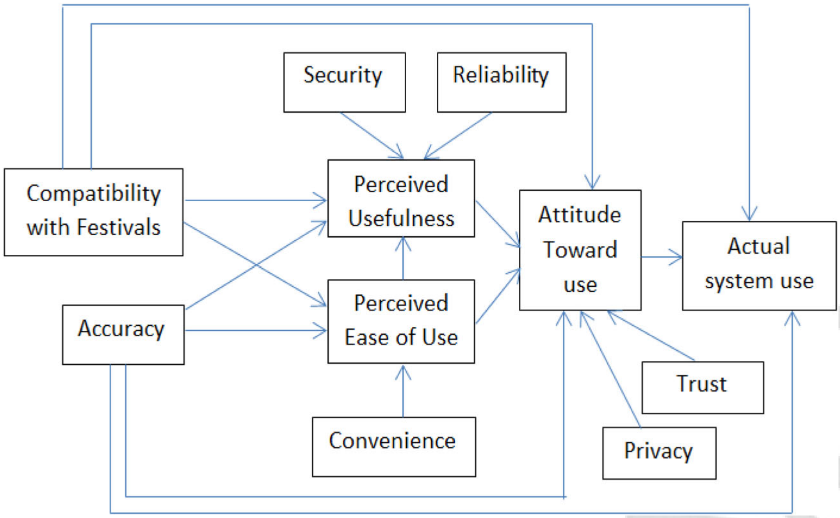

Figure 1. The studies amended TAM model.

Teolis, & Todd, 2005) to smartphone acceptance during leisure-based tourism (O'Regan & Chang, 2015). However, the original TAM model has been criticized for its generalizability and failure to sufficiently predict in specific contexts and circumstances. That has provided an impetus for studies of BT to extend and adapt the model (Al-Harby, 2010; Alsamydai, 2014; Ami-Narh, Aziale, & Akanferi, 2014; Holden & Karsh 2010; James, Pirim, Boswell, Reithel, & Barkhi, 2006; Miltgen et al., 2013; Morosan, 2012b; Tassabehji & Kamala, 2009; Sumner, 2007). Adding additional factors or combining the model with other acceptance models can enhance the TAM specificity and explanatory utility (Szajna, 1996). While researchers have extended the TAM model by adding variables such as consumer perceptions (Moore & Benbasat, 1991), and gender (Gefen & Straub, 1997), TAM studies related to BT acceptance have included variables such as concern for information privacy and voluntariness (Elgarah & Falaleeva, 2005), accuracy, security, and trust (Ngugi, Kamis, & Tremaine, 2011) and facilitating conditions, innovativeness, social influence and perceived risks (Miltgen et al., 2013). This study adapts an a TAM proposed by Ho et al. (2003), which itself is derived from an extended TAM by Venkatesh and Davis (2000) to create a conceptual model (Figure 1) to understand the issues surrounding BT adoption at festivals.

The model uses two key determinants—perceived usefulness and perceived ease of use—based on the TAM, and additional factors based on the extant literature and researcher knowledge of the festival sector. The model follows the TRA in selecting respondent's attitudes toward use and actual use as dependent variables (Table 2).

Dependent and independent variables

Attitude toward use (ATU)

Within the model, Attitude to Use (ATU) includes privacy and trust. While Ho et al. (2003) originally favored the variable "intention to use," attendees at a festival may not have the option of using the technology. Therefore ATU is a more appropriate variable. The relationship between ATU and privacy, trust, accuracy, compatibility, perceived usefulness (PU) and perceived ease of use (PEOU) has been hypothesized as:

H1. Privacy positively affects the ATU

H2. Trust positively affects the ATU

H3. Accuracy positively affects the ATU

H4. Compatibility positively affects the ATU

H5. PU positively affects the ATU

H6. PEOU positively affects the ATU

Perceived usefulness (PU)

Saade and Bahli (2005, p. 318) define perceived usefulness as "the degree to which a person believes that using a particular system could enhance his or her job performance." Perceived usefulness is a strong determinant of users' adoption and behavior, and within the study contest, indicates how useful a festival goer finds the technology in the festival context. Ho et al. (2003) argues that security, accuracy, cost, information sensitivity and reliability are determinants of perceived usefulness. The study model includes security and reliability as variables. Reliability refers to the probability that the system does not fail in achieving its intended outcomes (Chau, Stephens, & Jamieson, 2004). Whilst there have been few TAM studies incorporating the variable (Moon, Kang, Choi, & Kim, 2015), the literature indicates that reliability of a biometric modality, regardless of factors such as environment, age, ethnicity, and skin integrity, is important at a large population event like a festival. The extant literature also regards security as a significant factor, with Ho et al. (2003, p. 3) noting that security refers to "the confidentiality, integrity and availability of information used" (Ho et al., 2003). The relationship between PU and PEOU, security, reliability, compatibility and accuracy has been hypothesized as:

Table 2. Questions and variables.

Variable	Question
Compatibility with Festivals	BT is suitable in the festival context I feel that authentication through biometric technology is compatible with my needs (Happel, 2017)
Accuracy	BT may not identify my identity correctly (Sumner, 2007) BT has high identification accuracy
Perceived usefulness (PU)	BT would improve the quality of the festival experience BT would make entering the festival easier BT would be useful at festivals (Davis, 1993)
Safety	BT would increase the security of festivals I would be more likely to attend a festival using biometrics knowing it will increase safety
Reliability	BT wouldn't work properly, affecting my festival experience BT is more reliable than other traditional security methods (Lease, 2005)
Perceived ease of use (PEOU)	BT is simple as I would not be required to bring paper/ electronic tickets (Huys, 2014) BT would be easy for me to use (Alharbi & Drew, 2014) BT would be clear and understandable to interact with (Davis, 1993)
Convenience	BT would make the festival processes and interactions more convenient BT requires little effort or work (Huys, 2014)
Attitude toward use - ATU	I want to use biometric technology at festivals Is a positive idea (Alharbi & Drew, 2014)
Trust	I would trust these systems (Huys, 2014)
Privacy	BT could be used to steal my identity BT ensures that my personal information is well protected (Huys, 2014)
Actual Use - AU	I would attend a festival using biometric technology

H7. PEOU positively affects the PU

H8. Security positively affects the PU

H9. Reliability positively affects the PU

H10. Compatibility positively affects the PU

H11. Accuracy positively affects the PU

Perceived ease of use (PEOU)

PEOU is defined by Davis (1989a, p. 320) as "the degree to which a person believes that using a particular system would be free of effort." In the conceptual model, PEOU and convenience have been included as variables, with Ho et al. (2003) noting that convenience can be a significant determinant of PEOU. As convenience means a user's preference for convenient products and services, Hsu and Chang (2013) found that perceived convenience of an online system has a positive effect on perceived usefulness. The relationship between PEOU and accuracy, compatibility and convenience has been hypothesized as:

Table 3. ATU hypothesis results.

Hypothesis	Coefficient	*P* value	Result
H1. Privacy – ATU	−0.1232309	0.729	Retain the null hypothesis
H2. Trust – ATU	1.334464	0.001	Reject the null hypothesis
H3. Accuracy – ATU	−0.2811234	0.383	Retain the null hypothesis
H4. Compatibility – ATU	1.653471	0.000	Reject the null hypothesis
H5. PU – ATU	0.070985	0.837	Retain the null hypothesis
H6. PEOU – ATU	1.389354	0.000	Reject the null hypothesis

H12. Accuracy positively affects the PEOU

H13. Compatibility positively affects the PEOU

H14. Convenience positively affects the PEOU

Actual use (AU)

Actual use (AU) was used by Davis et al. (1989b) in the original TAM model, and is a well-established dependent variable (Ho et al., 2003).The relationship between AU and ATU, compatibility and accuracy has been hypothesis as:

H15. ATU positively affects the AU

H16. Compatibility positively affects the AU

H17. Accuracy positively affects the AU

The hypotheses were tested on data collected from a self-administrated questionnaire. The initial section consisted of screening questions to ensure the study participants were United Kingdom residents aged between 18 and 25 years, and had previously been to an outdoor music festival. The questionnaire provided respondents with an explanation (using illustrations) of facial recognition, iris scanning and fingerprint recognition, and asked the respondents about their previous knowledge of BT. TAM items were measured on a seven Likert-scale (1 = Definitely disagree, 7 = Definitely agree). Prior to designing the survey instrument, the questionnaire was piloted to 13 people, and 8 amendments were made to improve the clarity and meaning of the statements. The questionnaires were completed anonymously to reduce self-report bias and "opt-in consent" was requested. The questionnaire was administered online using Google Forms and was available from the 15th February 2018 until the 24th February 2018. Promoted via social media, a total of 127 completed responses were collected through a mixture

Table 4. Perceived usefulness hypothesis results.

Hypothesis	Coefficient	*P* value	Result
H7. PEOU – PU	0.62884	0.004	Reject the null hypothesis
H8. Security – PU	0.4995144	0.027	Reject the null hypothesis
H9. Reliability – PU	−0.1993174	0.461	Retain the null hypothesis
H10. Compatibility – PU	0.8880573	0.000	Reject the null hypothesis
H11. Accuracy – PU	−0.2671012	0.253	Retain the null hypothesis

of convenience and purposeful sampling (Etikan, Musa, & Alkassim, 2016). This data was analyzed using S.P.S.S 22 and Stata 12. The Cronbach Alpha Test was applied on S.P.S.S to get a better understanding of the validity and reliability of the 22 Likert-scale questions. The TAM statements had a Cronbach Alpha score of .945, indicating factor reliability (Gliem & Gliem, 2003). The study employed Stata software version 12 to empirically validate the conceptual model through Ordered Logistic Regression (OLR). When choosing between regression methods, the primary statistical principle it that it should fit the data and not vice versa (Berenson & Levine, 1992). Based on the characteristics of the data, the most optimal method was chosen to perform the analysis. OLR was suitable because it works well on small samples (Fullerton, 2009), is a well-established methodological procedure in TAM studies (Kolodinsky, Hogarth, & Hilgert, 2004; Lee & Kim, 2014) and can be used to test hypotheses (Murad, Fleischman, Sadetzki, Geyer, & Freedman, 2003). In order to analyze OLR data, the constant variables (PU, PEOU, ATU and AU) were reduced to three points on the Likert scale (disagree, neither agree nor disagree and agree) instead of seven points. One to three (Definitely disagree, disagree, and mostly disagree) was reduced to 1 point (Disagree), 4 (neither agree nor disagree) was turned to 2 (neither agree nor disagree), 5–7 (mostly agree, agree and definitely agree) was reduced to 1 point (Agree). In order to analyze the data, each question was grouped into a variable (Table 2), and the mean responses were used as the basis for the study. The level of critical significance was assigned at $p < 0.05$ (Vaske, 2008).

Findings

The data analysis shows that 67.2% of the respondents were female and 32% were male. While 44% of respondents had heard of the term biometrics before, 54.4% had not. 40.8% of the sample was employed, and 57.6% were students, with the remaining 1.6% either self-employed or not employed. Other findings identified that 70.9% of the respondents would feel comfortable using fingerprint recognition at music festivals, 68.5% with facial recognition and 50.4% would feel comfortable using iris scanning. After testing the conceptual model, ATU hypothesis (Table 3) results show that H1 and H3 had a negative and insignificant relationship between

Table 5. Perceived ease of use hypothesis results.

Hypothesis	Coefficient	*P* value	Result
H12. Accuracy – PEOU	0.7674734	0.001	Reject the null hypothesis
H13. Compatibility – PEOU	0.4795256	0.008	Reject the null hypothesis
H14. Convenience - PEOU	1.006646	0.000	Reject the null hypothesis

privacy, accuracy and the ATU, and therefore null hypothesis is retained. H2, H4 and H6 displayed a significant and positive relationship between trust, compatibility, PEOU and the ATU. Therefore the null hypothesis is rejected. Finally H5 showed a positive but insignificant relationship between PU and the ATU and therefore the null hypothesis is retained.

Importantly, hypothesis two results reveal that trust positively affects the attitude to use BT at festivals. Secondly, hypothesis four results reveal that compatibility positively affects the attitude to use biometrics at festivals. Finally, hypothesis six results reveal that the perceived ease of use positively affects the attitude to use biometrics at festivals. These results therefore indicate that trust, compatibility and perceived ease of use positively affect the attitude to use biometrics at festivals.

The results of the OLR (Table 4) indicate that H7, H8 and H10 had a positive and significant relationship between PEOU, security, compatibility and the PU and therefore reject the null hypothesis. H9 and H11 showed that there was a negative and insignificant relationship between reliability, accuracy and PU and therefore the null hypothesis is retained. Importantly, hypothesis seven results reveal that the perceived ease of use positively affects the perceived usefulness of biometrics at festivals. Hypothesis eight results reveal that security positively affects the perceived usefulness at festivals. Finally, hypothesis ten results reveal that the compatibility positively affects the perceived usefulness of biometrics at festivals.

The results of the OLR indicate that H12, H13 and H14 (Table 5) had a positive and significant relationship between accuracy, compatibility, convenience and PEOU and therefore the null hypothesis is rejected. Importantly, hypothesis twelve results reveal that the accuracy positively affected the perceived ease of use of biometrics. Hypothesis thirteen results reveal that compatibility positively affected the perceived ease of use of biometrics and finally hypothesis fourteen results reveal that convenience positively affected the perceived ease of biometrics. These results therefore indicate that perceived ease of use, security and compatibility positively affect the perceived usefulness of biometrics at festivals and accuracy, compatibility and convenience positively affect the perceived ease of use of biometrics at festivals.

The results of the OLR (Table 6) indicated that H15 and H17 had a positive and significant relationship between the ATU, accuracy and the AU and therefore reject the null hypothesis. H16 had a positive but

Table 6. Actual use of use hypothesis results.

Hypothesis	Coefficient	*P* value	Result
H15. ATU – AU	1.851002	0.000	Retain the null hypothesis
H16. Compatibility – AU	0.485429	0.104	Reject the null hypothesis
H17. Accuracy – AU	0.7023727	0.008	Retain the null hypothesis

insignificant relationship between compatibility and AU and therefore retain the null hypothesis. Importantly, hypothesis fifteen results reveal that the attitude to use biometrics at festivals positively affects the actual use. These results therefore indicate that attitude and accuracy positively affect the actual use of biometrics at festivals.

Discussion

This study found variables, such as convenience, trust, compatibility and security, were significant to respondents, and factors including reliability, accuracy and privacy were not. The accuracy of BT was found to have a significant relationship with perceived ease of use (PEOU). This is in line with results from Sidharta, Priadana, and Affandi (2016), who note that accuracy and timeliness have a significant impact on the PEOU. There was also a significant relationship between accuracy and perceived usefulness (PU). While this finding is supported in TAM studies (Langenderfer & Linnhoff, 2005), Murphy and Rottet (2009) specifically found accuracy to be a particular concern to BT users. However, the study unexpectedly found that accuracy had no significant relationship with attitude to use (ATU) and actual use (AU). The findings suggest respondents would be willing to trade away accuracy for attendance, at least in the festival context, where misidentification may not be perceived as leading to serious consequences. Given that there is some evidence to suggest that older consumers avoid risk and prefer accuracy in technology adoption (Jia, Lu, & Wajda, 2015), young adults may be willing to accept BT at a festival, despite issues with BT accuracy. This is concerning, as facial recognition systems have been found to misidentify people of color more often than white people, and inaccurate identification may lead to harassment, and even detainment of innocent attendees. It could for example, lead some attendees to be refused festival entry. Privacy was identified in the literature as having a strong effect on the core TAM constructs, such as attitude, behavioral intention, and use behaviors related to BT (Liu & Silverman, 2001; Giesing, 2005; Morosan, 2012a). However, unexpectedly, privacy was not found to have a significant impact on the ATU. This may indicate that privacy amongst young adults, used to sharing information, may not be foremost in their minds. Given festival attendance and entry, along with other functions, may be conditional on BT use, young adults may feel compelled to accept BT. Similar tradeoffs amongst young adults have been found with Instagram (Doleck, Bazelais, & Lemay, 2017) and Snapchat use and acceptance (Lemay, Doleck, & Bazelais, 2017). This finding goes against the popular narrative that privacy is an important factor in the acceptance and use of BT. This is a concerning result, given data might be shared with authorities and external parties, and could, for example, lead to the arrest of attendees on outstanding criminal charges.

Convenience was found to have a positive impact on the PEOU, with young adults showing a strong preference for convenience. The respondents believe BT will make their lives easier (Hsu & Chang, 2013; Yoon & Kim, 2007). Frumkin (2015) remarked that the millennial generation are also known as convenience customers, who enjoy innovative technology, but may stop using if they believe that they are putting in too much effort to use it. Trust, was found to have a significant impact on the ATU. Given that studies find that consumers have trust issues with BT (Giesing, 2003; Morosan, 2012a), a lack of trust in a technology would act as a potential obstacle to its acceptance (Bélanger & Carter, 2008). The finding is supported by studies which found trust has a significant impact on the ATU (Ha & Stoel, 2009; Hassanein & Head, 2007; Tung, Chang, & Chou, 2008). The findings indicate that trust needs to be maintained by BT providers and those who utilize it, since trust can be easily lost. In line with extant literature, the study found that compatibility had a significant relationship with ATU and PEOU (Lane & Stagg, 2014; Miltgen et al., 2013). The relationships are situational, with Chen, Yen, and Chen (2009) finding no relationship between compatibility and ATU and PEOU with regards to smart phone use. Compatibility can play an essential role in BT adoption, as it indicates BT is perceived to be consistent with the respondent's beliefs, lifestyle, values and past experience. However, this study found no significant relationship between compatibility and PU. This may indicate that respondent's preferred festival practices, or prior experiences with BT at festivals have yet to trigger positive perception of the use value of BT at a festival setting (Karahanna, Agarwal, & Angst, 2006). In line with extant literature, the study found that security has a positive effect on PU (Trocchia & Ainscough, 2006; Westdorp, 2015; Yoon & Steege, 2013). Since personal data can be intercepted and used for fraudulent purposes, BT requires security safeguards, and attendees may need security guarantees. Respondents need a sense of security to accept BT, so as to reduce subjective risk perception. Security mechanisms to reduce the objective and subjective risks will lead to an increased effect on its PU. While reliability, in regards to BT has been identified as important in the literature (Deane, Barrelle, Henderson, & Mahar, 1995; Fairhurst, 1997; Morosan, 2012b), this study found that reliability was not a significant factor for 18–25 year olds.

This indicates that reliability will not affect PU of the technology, with individuals continuing to use BT regardless.

The study found that the PEOU of BT had a significant impact on the PU and ATU of BT. Davis (1993) found that PEOU had a strong influence on PU, and this was also confirmed by Morosan (2012b), Jones, McCarthy, Halawi, and Mujtaba (2010), and Jain et al. (2008). The PEOU positively affecting the ATU was also supported by Morosan (2012b), Al-Harby, Qahwaji, and Kamala (2009), and Lane and Stagg (2014). In line with extant literature, ATU was identified as having a significant impact on the AU of BT (Al-Harby et al., 2009; Davis, 1993; Morosan, 2012b; Ko, 2014). PU did not have a significant effect on ATU, despite empirical support for the relationship. While extant literature found a significant relationship between the PU and ATU in the acceptance of BT (Al-Harby, 2010; Morosan, 2012b; Lane & Stagg, 2014; Yu, Ha, Choi, & Rho, 2005), PU was not found to be a critical factor in particular contexts, such as a Library Automation System (Hak, 2015), and a e-learning system (Al-Adwan, Al-Adwan, & Smedley, 2013). It is an important finding given the PU variable is the most significant and important variable in influencing attitudes to use a technology (Davis, 1989a; Sun, 2003). The PU generated by BT, offers, at least in the perception of respondents, no effect on user acceptance. Instead, it seems acceptance is based primarily on convenience, and security.

The study findings indicate that festival attendees may be willing to "opt in" to BT, as long as it's explained how the technology works for them. Attendees will need to perceive benefits from BT, and festival organizers will need to provide information that describes the usefulness of BT as well focus attention of the convenience, and security of their BT systems. This will allow event goers to develop positive attitudes toward use. While it was expected that the accuracy, reliability and privacy may be significance to users, the study found that security and convenience are more important factors in contributing to consumers' intention to accept BT at festivals. Whilst the findings suggest that necessity beliefs outweigh concerns and have strong effects on acceptance and use, festival organizers may still be reluctant to adopt BT, despite the willingness and acceptance amongst young adults. As BT becomes more common, privacy needs to be balanced with security. Whilst attendees seem willing to trade privacy and accuracy for use, organizers will need to address those in the community, authorities and other stakeholders, such as parents, who may raise the concern that festivals are being co-opted as sites for the normalization of a far-reaching technology. As legislation has trailed the adoption of BT, festival organizers need to ensure basic rights are being ensured and data is protected. This may mean giving attendees the option to opt in and ensure data is not retained in databases after the festival end. For example, whilst an attendee might be happy to trade their picture and registration number for entry, other identifying information, such as email address and birth date should be secured, with the whole database deleted after the event.

Festival organizers will need to clear as to their intentions, justifications for use, and the usefulness of BT to attendees, artists, regulators and authorities. BT could in practice be used to identify and deport illegal immigrants, match faces with home address and ticket purchase details, match faces with custody images from across Europe and lead to the arrest of attendees for past offenses, or minor offenses committed at the festival. If young adults do not have knowledge or understand the important role of accuracy and privacy, organizers must develop a governance framework to ensure transparency and accountability around BT use. Just as the Association of Independent Festivals (AIF) (2019) have developed a charter of best practice on sexual assault at festivals, a similar code of conduct is required for BT use in the UK. If festival organizers do not create pathways toward greater education and acceptance by multiple stakeholders, including artists and promoters, digital rights advocacy groups might step in. In the United States, the Fight For the Future group, for example, has released a list of music festivals that have pledged to never employ BT for ticketing or security purposes at their events, and organized a petition (www.banfacialrecognition.com/festivals/) against BT. Finally, organizers should carefully consider all stakeholders before utilizing COVD-19 and sanitation to justify the introduction of BT at festivals.

Conclusions

The study found that festival goers would accept and use BT at music festivals. Contrary to expectations, BT acceptance and use is driven less by accuracy, reliability and privacy, and more by security and convenience. This goes against the popular narrative that accuracy, reliability and privacy are important factors in the adoption and use of BT. While the study suggests that privacy may not be operative in the liminal festival context for young adults, the findings raises ethical questions for event organizers, authorities, parents, artists, police services and biometric companies when contemplating the introduction of such systems for use in the events sector. As young adults seem to be immune to the risks associated with BT, festival organizers need to take on additional educational, outreach and data protection responsibilities.

Limitations and suggestions for future research

The findings cannot accurately represent the acceptance of BT amongst older festival attendees, who may have a greater aversion to BT. The study did not consider diversity in the United Kingdom and the ways in which underrepresented minorities may come to accept and use BT. The model should sample attendees in different countries, and cultural contexts, to generalize its findings. Further studies should study acceptance amongst festival workers, traders, artists and promoters. As TAM generally explains between 40% and 60% of variance in use, there are likely other constructs and path relationships that could be involved in acceptance and use behaviors (Lemay et al., 2017). Finally, whilst this studies data analysis is statistically relevant, future studies should increase sample size, especially when incorporating Ordered Logistic Regression (OLR).

References

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

Al-Adwan, A., Al-Adwan, A., & Smedley, J. (2013). Exploring students' acceptance of e-learning using technology acceptance model in Jordanian universities. *International Journal of Education and Development Using ICT*, *9*(2), 4–18.

Al-Harby, F., Qahwaji, R., & Kamala, M. (2009). *The effects of gender differences in the acceptance of biometrics authentication systems within online transaction*. In Proceedings of the International Conference on CyberWorlds, IEEE, pp. 203–210.

Q5

Al-Harby, F. M. (2010). *Biometric authentication systems for secured e-transactions in Saudi Arabia. An empirical investigation of the factors affecting users' acceptance of fingerprint authentication systems to improve online security for e-commerce and e-government websites in Saudi Arabia* (Doctoral dissertation). University of Bradford.

Alharbi, S., & Drew, S. (2014). Using the technology acceptance model in understanding academics' behavioural intention to use learning management systems. *International Journal of Advanced Computer Science and Applications*, *5*(1), 143–155. doi:10.14569/IJACSA.2014.050120

Alsamydai, M. J. (2014). Adaptation of the technology acceptance model (TAM) to the use of mobile banking services. *International Review of Management and Business Research*, *3*(4), 2039–2051.

Ami-Narh, J. T., Aziale, L. K., & Akanferi, A. A. (2014). The adoption of biometric technology in the Ghanaian business community – effectiveness and impact. *International Journal of Computer Applications*, *85*(9), 32–39. doi:10.5120/14871-3246

Arbon, P. (2004). The development of conceptual models for mass-gathering health. *Prehospital and Disaster Medicine*, *19*(3), 208–212. doi: 10.1017/S1049023X0000179

Association of Independent Festivals. (2019). Sexual assault at festivals: AIF charter of best practice. Retrieved from https://aiforg.com/wp-content/uploads/Charter-of-Best-Practice-Final.pdf

Aviva. (2012). UK: Cover yourself with more than a tent at summer festivals. Aviva, June 20.

Bakir, V., Cable, J., Dencik, L., Hintz, A., & McStay, A. (2015). Public feeling on privacy, security and surveillance: A report by DATA-PSST and DCSS. [Project Report]. Cardiff University and Bangor University. Retrieved from https://dcssproject.net/public-feeling/

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, *17*(2), 165–176. doi:10.1016/j.jsis.2007.12.002

Berenson, M. L., & Levine, D. M. (1992). *Basic business statistics: Concepts and application*. New York, NY: Pentin Hall. Inc.

Bharadwaj, S., Vatsa, M., & Singh, R. (2014). Biometric quality: A review of fingerprint, iris, and face. *EURASIP Journal on Image and Video Processing*, *2014*(1), 34. doi:10.1186/1687-5281-2014-34

Bhatia, R. (2013). Biometrics and face recognition techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(2013), 5.

Bowdin, G., Allen, J., Harris, R., McDonnell, I., & O'Toole, W. (2012). *Events management*. Abingdon, UK: Routledge.

Boyle, P., & Haggerty, K. D. (2012). Planning for the worst: Risk, uncertainty and the Olympic Games. *The British Journal of Sociology*, *63*(2), 241–259. doi:10.1111/j.1468-4446.2012.01408.x

Brathwaite, R. (2017). What's biometric security and is my phone safe? *TSB Bank Plc*. Retrieved from https://www.tsb.co.uk/straightforward-money/whats-biometric-security-and-is-my-phone-safe/

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In Proceedings of the Conference on Fairness, Accountability and Transparency. *PMLR*, *81*, 77–91.

Buciu, I., & Gacsadi, A. (2016). Biometrics systems and technologies: A survey. *International Journal of Computers Communications & Control*, *11*(3), 315–330. doi:10.15837/ijccc.2016.3.2556

Cavoukian, A. (1999). *Consumer biometric applications: A discussion paper*. Toronto: Information and Privacy Commissioner.

CGA. (2019). Your future in festivals—How to stand out from the crowd. Retrieved from https://www.cga.co.uk/wp-content/uploads/2019/04/CGA-Your-Future-in-Festivals-How-to-stand-out-from-the-crowd.pdf

Chan, S. (2017). Facial recognition makes way into airport and other industries. *Cisco*. Retrieved from https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1834698

Chau, A., Stephens, G., & Jamieson, R. (2004). *Biometrics acceptance-perceptions of use of biometrics*. In Proceedings of the Australasian Conference on Information Systems (ACIS'04), pp. 1–6.

Chen, J. V., Yen, D. C., & Chen, K. (2009). The acceptance and diffusion of the innovative smart phone use: A case study of a delivery service company in logistics. *Information & Management*, *46*(4), 241–248. doi:10.1016/j.im.2009.03.001

Chowhan, S. S., & Shinde, G. N. (2008, May). *Iris biometrics recognition application in security management*. In Proceedings of the Congress on Image and Signal Processing, IEEE, pp. 661–665.

Clarke, N. L., Furnell, S. M., & Reynolds, P. L. (2002). *Biometric authentication for mobile devices*. In Proceedings of the 3rd Australian information warfare and security conference (INC2002), pp. 61–69.

Dai, S. (2018). Meet five Chinese start-ups pushing facial recognition technology into the mainstream. *South China Morning Post*. Retrieved from https://www.scmp.com/tech/start-ups/article/2133234/meet-five-chinese-start-ups-pushing-facial-recognition-technology

Davies, J. D. (2017). Are music festivals doing enough to tackle sexual assault? *The Guardian*, July 25. Retrieved from https://www.theguardian.com/lifeandstyle/2017/jul/25/music-festivals-sexual-assault-rape-safe

Davies, S. G. (1994). Touching Big Brother: How biometric technology will fuse flesh and machine. *Information Technology & People*, *7*(4), 38–47. doi:10.1108/095938494100

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation). Massachusetts Institute of Technology. Q6

Davis, F. D. (1989a). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. doi:10.2307/249008

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies*, *38*(3), 475–487. doi:10.1006/imms.1993.1022

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989b). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. doi:10.1287/mnsc.35.8.982

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science*, *48*(1), 28–46. doi:10.1111/j.0092-5853.2004.00054.x

Deane, F., Barrelle, K., Henderson, R., & Mahar, D. (1995). Perceived acceptability of biometric security systems. *Computers & Security*, *14*(3), 225–231. doi:10.1016/0167-4048(95)00005-S

Dee, C. R., Teolis, M., & Todd, A. D. (2005). Physicians' use of the personal digital assistant (PDA) in clinical decision making. *Journal of the Medical Library Association*, *93*(4), 480–486.

Delac, K., & Grgic, M. (2004, June). *A survey of biometric recognition methods*. In Proceedings of the 46th International Symposium on Electronics in Marine (Elmar-2004), pp. 184–193.

Doleck, T., Bazelais, P., & Lemay, D. J. (2017). Need for self-expression on instagram: A technology acceptance perspective. In Proceedings of the 3rd International Conference on Computational Intelligence & Communication Technology (CICT), IEEE, pp. 1–3.

Down, M. P., & Sands, R. J. (2004). Biometrics: An overview of the technology, challenges and control considerations. *Information Systems Control Journal*, *4*, 53–56.

Elgarah, W., & Falaleeva, N. (2005). *Adoption of Biometric Technology: Information Privacy in TAM*. In Proceedings of the Americas Conference on Information Systems (AAMCIS 2005), pp. 1209–1212.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1–4. doi:10.11648/j.ajtas.20160501.11

Fairhurst, M. C. (1997). Signature verification revisited: Promoting practical exploitation of biometric technology. *Electronics & Communication Engineering Journal*, *9*(6), 273–280. doi:10.1049/ecej:19970606

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Frumkin, T. (2015). Why millennials are the convenience generation. *Salesforce*, June 1. Retrieved from https://www.salesforce.com/blog/2015/06/why-millennials-convenience-generation.html

Fullerton, A. S. (2009). A conceptual framework for ordered logistic regression models. *Sociological Methods & Research*, *38*(2), 306–347. doi:10.1177/0049124109346162

Galbally, J., Marcel, S., & Fierrez, J. (2014). Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Transactions on Image Processing*, *23*(2), 710–724. doi:10.1109/TIP.2013.2292332

Garg, N., & Singh, S. (2014). Biometric technology—A review. *International Journal of Enhanced Research in Science Technology & Engineering*, *3*(3), 296–299.

Gefen, D., & Straub, D. W. (1997). Gender differences in the perception and use of e-mail: An extension to the technology acceptance model. *MIS Quarterly*, *21*(4), 389–400. doi:10.2307/249720

Giesing, I. (2005). *User perceptions related to identification through biometrics within electronic business* (Doctoral dissertation). University of Pretoria.

Gisbert, V., & Rius-Ulldemolins, J. (2019). Women's bodies in festivity spaces: Feminist resistance to gender violence at traditional celebrations. *Social Identities*, *25*(6), 775–718. doi:10.1080/13504630.2019.1610376

Gliem, J. A., & Gliem, R. R. (2003). *Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales*. In Proceedings of the Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education, Ohio State University, Columbus, OH, pp. 82–88.

Ha, S., & Stoel, L. (2009). Consumer e-shopping acceptance: Antecedents in a technology acceptance model. *Journal of Business Research*, *62*(5), 565–571. doi:10.1016/j.jbusres.2008.06.016

Hak, A. A. (2015). An analysis of the acceptance's staffs of Madrassa Library on 'Senayan'-based library automation system using technology acceptance model (TAM). Library Philosophy and Practice. Retrieved from https://digitalcommons.unl.edu/libphilprac/1260/

Halevi, T., Kuppusamy, T. K., Caiazzo, M., & Memon, N. (2015). *Investigating users' readiness to trade-off biometric fingerprint data*. In Proceedings of the International Conference on Identity, Security and Behavior Analysis (ISBA 2015), IEEE, pp. 1–8. doi:10.1109/ISBA.2015.7126366

Hamid, L. (2015). Biometric technology: Not a password replacement, but a complement. *Biometric Technology Today*, *2015*(6), 7–10. doi:10.1016/S0969-4765(15)30097-7

Hanumanthappa, M., LourdhuSuganthi, S. R., & Karthik, S. (2015). Tagging event image set using face identification. In Proceedings of the International Conference on Soft-Computing and Networks Security (ICSNS), IEEE, pp. 1–5. doi:10.1109/ICSNS.2015.7292377

Happel, B. L. (2017). *What' you are to show 'who' you are: User acceptance of biometrics in eHealth video consultants* (Masters dissertation). Radboud University.

Hassanein, K., & Head, M. (2007). Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *International Journal of Human-Computer Studies*, *65*(8), 689–708. doi:10.1016/j.ijhcs.2006.11.018

Holden, R. J., & Karsh, B. T. (2010). The technology acceptance model: Its past and its future in health care. *Journal of Biomedical Informatics*, *43*(1), 159–172. doi:10.1016/j.jbi.2009.07.002

Ho, G., Stephens, G., & Jamieson, R. (2003). *Biometric authentication adoption issues*. In Proceedings of the 14th Australasian Conference on Information Systems, Hobart, Tasmania, Australia, pp. 1–6.

Hsu, H. H., & Chang, Y. Y. (2013). Extended TAM model: Impacts of convenience on acceptance and use of moodle. *US-China Education Review A*, *3*(4), 211–218.

Huys, H. (2014). *Consumer acceptance of identification technology* (Doctoral dissertation). Ghent University.

IBM Security. (2018). *IBM Security: Future of identity study*. Cambridge, MA: IBM Security.

Jain, A., & Kumar, A. (2012). Biometric recognition: An overview. In E. Mordini & D. Tzovaras (Eds.), *Second generation biometrics: The ethical, legal and social context* (pp. 49–79). Dordrecht: Springer.

Jain, A., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern Recognition*, *38*(12), 2270–2285. doi:10.1016/j.patcog.2005.01.012

Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advances in Signal Processing*, *2008*(1), 579416. doi:10.1155/2008/579416

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 4–20. doi:10.1109/TCSVT.2003.818349

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. *Journal of Organizational and End User Computing*, *18*(3), 1–24. doi:10.4018/joeuc.2006070101

Jia, P., Lu, Y., & Wajda, B. (2015). Designing for technology acceptance in an ageing society through multi-stakeholder collaboration. *Procedia Manufacturing*, *3*, 3535–3542. doi:10.1016/j.promfg.2015.07.701

Jones, C. M., McCarthy, R. V., Halawi, L., & Mujtaba, B. (2010). Utilizing the technology acceptance model to assess the employee adoption of information systems security measures. *Issues in Information Systems*, *11*(1), 9.

Juniper Research. (2017). Mobile biometric payment volumes to triple in 2017 to nearly 2BN. Hampshire: Juniper Research Ltd. Retrieved from https://www.juniperresearch.com/press/press-releases/mobile-biometric-payment-volumes-to-triple-in-2017

Karahanna, E., Agarwal, R., & Angst, C. M. (2006). Reconceptualizing compatibility beliefs in technology acceptance research. *MIS Quarterly*, *30*(4), 781–804. doi:10.2307/25148754

Kavanagh, M. M., Baral, S. D., Milanga, M., & Sugarman, J. (2019). Biometrics and public health surveillance in criminalised and key populations: Policy, ethics, and human rights considerations. *The Lancet Hiv*, *6*(1), e51–e59. doi:10.1016/S2352-3018(18)30243-1

Ko, C.H. (2014). Exploring employees' perceptions of biometric technology adoption in hotels. *Biotechnology: An Indian Journal*, *10*(21), 13242–13246.

Kolodinsky, J. M., Hogarth, J. M., & Hilgert, M. A. (2004). The adoption of electronic banking technologies by US consumers. *International Journal of Bank Marketing*, *22*(4), 238–259. doi:10.1108/02652320410542536

Lane, M. S., & Stagg, A. (2014). University staff adoption of iPads: An empirical study using an extended TAM model. *Australasian Journal of Information Systems*, *18*(3). doi:10.3127/ajis.v18i3.876

Q7

Langenderfer, J., & Linnhoff, S. (2005). The emergence of biometrics and its effect on consumers. *Journal of Consumer Affairs*, *39*(2), 314–338. doi:10.1111/j.1745-6606.2005.00017.x

Lawson, W. J. (2003). *Enhancing assistive technologies: Through the theoretical adaptation of biometric technologies to people of variable abilities* (Doctoral dissertation). Kennedy-Western University.

Lease, D. R. (2005). *Factors influencing the adoption of biometric security technologies by decision making information technology and security managers* (Doctoral dissertation). Capella University.

Lee, J., & Kim, S. (2014). Active citizen e-participation in local governance: Do individual social capital and e-participation management matter?. In *Proceedings of the 47th Hawaii International Conference on System Sciences*, *IEEE*, 2044–2053. doi:10.1109/HICSS.2014.259

Lemay, D. J., Doleck, T., & Bazelais, P. (2017). Passion and concern for privacy' as factors affecting snapchat use: A situated perspective on technology acceptance. *Computers in Human Behavior*, *75*, 264–271. doi:10.1016/j.chb.2017.05.022

Liu, I. F., Chen, M. C., Sun, Y. S., Wible, D., & Kuo, C. H. (2010). Extending the TAM model to explore the factors that affect intention to use an online learning community. *Computers & Education*, *54*(2), 600–610. doi:10.1016/j.compedu.2009.09.009

Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. *IT Professional*, *3*(1), 27–32. doi:10.1109/6294.899930

Lui, J., & Xiqing, W. (2017). In Your Face: China's all-seeing state. *BBC News*. Retrieved from http://www.bbc.co.uk/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state

Martin, A. J. (2017). Police facial recognition trial led to 'erroneous arrest'. *Sky News*, September 7. Retrieved from https://news.sky.com/story/police-facial-recognition-trial-led-to-erroneous-arrest-11013418

Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials*, *17*(3), 1268–1293. doi:10.1109/COMST.2014.2386915

Millward, D. (2016). Police warn of terror threat to music festivals. *The Telegraph*, May 26. Retrieved from https://www.telegraph.co.uk/news/2016/05/29/police-warn-of-terror-threat-to-music-festivals-and-sporting-eve/

Miltgen, C. L., 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*, 103–114. doi:10.1016/j.dss.2013.05.010

Mintel. (2017). *Music concerts and festivals – UK – August 2017*. London: Mintel Group. Retrieved from https://store.mintel.com/uk-music-concerts-and-festivals-market-report

Mintel. (2019). *Music concerts and festivals – UK – August 2019*. London: Mintel Group. Retrieved from https://www.mintel.com/press-centre/leisure/raving-mad-uk-music-festival-attendance-at-highest-level-in-four-years

Moon, T., Kang, S., Choi, S., & Kim, D. (2015). Technology acceptance and perceived reliability of realistic media service. *Advanced Science and Technology Letters*, *8*(25), 105–111. doi:10.14257/astl.2015.113.22

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192–222. doi:10.1287/isre.2.3.192

Morosan, C. (2011). Customers' adoption of biometric systems in restaurants: An extension of the technology acceptance model. *Journal of Hospitality Marketing & Management*, *20*(6), 661–690. doi:10.1080/19368623.2011.570645

Morosan, C. (2012a). Biometric solutions for today's travel security problems. *Journal of Hospitality and Tourism Technology*, *3*(3), 176–195. doi:10.1108/17579881211264

Morosan, C. (2012b). Theoretical and empirical considerations of guests' perceptions of biometric systems in hotels: Extending the technology acceptance model. *Journal of Hospitality & Tourism Research*, *36*(1), 52–84. doi:10.1177/1096348010380601

Murad, H., Fleischman, A., Sadetzki, S., Geyer, O., & Freedman, L. S. (2003). Small samples and ordered logistic regression: Does it help to collapse categories of outcome? *The American Statistician*, *57*(3), 155–160. doi:10.1198/0003130031892

Murphy, H. C., & Rottet, D. (2009). An exploration of the key hotel processes implicated in biometric adoption. *International Journal of Contemporary Hospitality Management*, *21*(2), 201–212. doi:10.1108/0959611091093

Nandakumar, K., Nagar, A., & Jain, A. K. (2007). Hardening fingerprint fuzzy vault using password. In Proceedings of the International Conference on Biometrics, Seoul, South Korea, pp. 927–937.

National Research Council & Whither Biometrics Committee. (2010). *Biometric recognition: Challenges and opportunities*. Washington, DC: National Academies Press.

Ngugi, B., Kamis, A., & Tremaine, M. (2011). Intention to use biometric systems. *e-Service Journal: A Journal of Electronic Services in the Public and Private Sectors*, *7*(3), 20–46. doi:10.2979/eservicej.7.3.20

Nilsson, P. (2018). How UK police are using facial recognition software, *Financial Times*, October 12. Retrieved https://www.ft.com/content/06c46942-cc7d-11e8-b276-b9069bde0956

Normalini, M. K., & Ramayah, T. (2017). Trust in internet banking in Malaysia and the moderating influence of perceived effectiveness of biometrics technology on perceived privacy and security. *Journal of Management Sciences*, *4*(1), 3–26. doi:10.20547/jms.2014.1704101

Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems*, *106*, 1–14. doi:10.1016/j.dss.2017.11.003

O'Regan, M., & Chang, H. (2015). Smartphone adoption amongst Chinese youth during leisure-based tourism: Challenges and opportunities. *Journal of China Tourism Research*, *11*(3), 238–254. doi:10.1080/19388160.2015.1077181

Oyserman, D., Elmore, K., & Smith, G. (2012). Self, self-concept, and identity. In M. R. Leary & J. P. Tangney (Eds.), *Handbook of self and identity* (pp. 69–104). New York, NY: Guilford Press.

Patel, R., & Yagnik, S. B. (2013). A literature survey on face recognition techniques. *International Journal of Computer Trends and Technology (IJCTT)*, *5*(4), 189–194.

Perala, A. (2017). Facial recognition Nabs 25 wanted criminals at Chinese beer festival. *Find Biometrics*. Retrieved from https://findbiometrics.com/facial-recognition-beer-festival-409012/

Pons, A. P., & Polak, P. (2008). Understanding user perspectives on biometric technology. *Communications of the ACM*, *51*(9), 115–118. doi:10.1145/1378727.1389971

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, *1*(2), 33–42. doi:10.1109/MSECP.2003.1193209

Schreiber-Gregory, D. (2018). Logistic and linear regression assumptions: Violation recognition and control. Henry M Jackson Foundation, Paper 130.

Sidharta, I., Priadana, S., & Affandi, A. (2016). Extending end-user computing satisfaction on academic information systems. *Indian Journal of Science and Technology*, *9*(48), 1–5. doi:10.17485/ijst/2016/v9i48/90485

Stikeman, A. (2003). 10 breakthrough technologies. Massachusetts Institute of Technology: *MIT Technology Review*. Retrieved from http://www2.technologyreview.com/news/401765/biometrics/

Sumner, K. M. (2007). *Airport security: Examining the current state of acceptance of biometrics and the propensity of adopting biometric technology for airport access control* (Doctoral dissertation). University of Central Florida.

Szajna, B. (1996). Empirical evaluation of the revised technology acceptance model. *Management Science*, *42*(1), 85–92. doi:10.1287/mnsc.42.1.85

Taouche, C., Batouche, M. C., Berkane, M., & Taleb-Ahmed, A. (2014). Multimodal biometric systems. In Proceedings of the International Conference on Multimedia Computing and Systems (ICMCS), IEEE, pp. 301–308. doi:10.1109/ICMCS.2014.6911308

Tassabehji, R., & Kamala, M. A. (2009). Improving e-banking security with biometrics: Modelling user attitudes and acceptance. In Proceedings of the 3rd International Conference on New Technologies, Mobility and Security, IEEE, pp. 1–6. doi:10.1109/NTMS.2009.5384806

Trocchia, P. J., & Ainscough, T. L. (2006). Characterizing consumer concerns about identification technology. *International Journal of Retail & Distribution Management*, *34*(8), 609–620. doi:10.1108/0959055061067

Tung, F. C., Chang, S. C., & Chou, C. M. (2008). An extension of trust and TAM model with IDT in the adoption of the electronic logistics information system in HIS in the medical industry. *International Journal of Medical Informatics*, *77*(5), 324–335. doi:10.1016/j.ijmedinf.2007.06.006

Turris, S. A., & Lund, A. (2017). Mortality at music festivals: Academic and grey literature for case finding. *Prehospital and Disaster Medicine*, *32*(1), 58–63. doi:10.1017/S1049023X16001205

Uzoka, F. M. E., & Ndzinge, T. (2009). Empirical analysis of biometric technology adoption and acceptance in Botswana. *Journal of Systems and Software*, *82*(9), 1550–1564. doi:10.1016/j.jss.2009.04.041

Vaske, J. (2008). *Survey research and analysis: Applications in parks, recreation and human dimensions*. State College, PA: Venture Publishing.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204. doi:10.1287/mnsc.46.2.186.11926

Vulliamy, E. (2016). Music festivals on 'high alert' for terror attacks, say police. *The Independent*, May 29. Retrieved from https://www.independent.co.uk/news/uk/home-news/music-festivals-on-high-alert-for-terror-attacks-say-police-a7055011.html

Weaver, A. C. (2006). Biometric authentication. Computer Magazine., *39*(2), 96–97. doi:10.1109/MC.2006.47

Westdorp, J. (2015). *Factors influencing the baby boomers' intention to use domotics to live independently for longer* (Masters dissertation). University of Twente.

Woodward, J. D., Jr., Horn, C., Gatune, J., & Thomas, A. (2003). *Biometrics: A look at facial recognition*. Santa Monica, CA: RAND CORP.

Wu, J. H., & Wang, S. C. (2005). What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model. *Information & Management*, *42*(5), 719–729. doi:10.1016/j.im.2004.07.001

Yoon, C., & Kim, S. (2007). Convenience and TAM in a ubiquitous computing environment: The case of wireless LAN. *Electronic Commerce Research and Applications*, *6*(1), 102–112. doi:10.1016/j.elerap.2006.06.009

Yoon, H. S., & Steege, L. M. B. (2013). Development of a quantitative model of the impact of customers' personality and perceptions on Internet banking use. *Computers in Human Behavior*, *29*(3), 1133–1141. doi:10.1016/j.chb.2012.10.005

Yu, J., Ha, I., Choi, M., & Rho, J. (2005). Extending the TAM for a t-commerce. *Information & Management*, *42*(7), 965–976. doi:10.1016/j.im.2004.11.001