Factors Affecting the Adoption of Online Biometrics by the Internet User Community

Declan O'Sullivan

A dissertation submitted to the University of Dublin in partial fulfilment of the requirements for the degree of MSc in Management of Information Systems

2nd September, 2013

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: ____________________
Declan O'Sullivan
2nd September, 2013

Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed: ___________________

Declan O'Sullivan
2nd September, 2013

Acknowledgements

Special thanks to my supervisor Aideen Keaney who gave great advice and support throughout the dissertation and introduced me to the interesting world of statistics and of course, Andy Field. I would also like to thank Niamh Dunne who gave great advice throughout the last two years and invaluable advice when starting this dissertation. I would also like to thank my classmates, Sean, Neil and Vikas who were my teammates for a good part of the two year term, working as a cohesive team, we got through those assignments. I would also like to thank my siblings for their support with piloting the online questionnaire as well as my parents for their invaluable support throughout the two years.

Finally, I would like to thank my wife Naomi, who was a brilliant support throughout the duration of the course, provided invaluable advice on the questionnaire and dissertation and for being a great parent to our son. Last but certainly not least, I would like to thank my son Fionnán Rian (Baltazar) for being the most special craziest little dude that I know, your laugh is infectious and you just bring joy to everyone that meets you. You have made me the proudest Dad ever.

Abstract

Biometric technologies have been slow to make their way online but this is about to change due to renewed interest and investment by corporations such as Apple and the need to stop and reverse the growth in identify theft related crimes. Online biometrics is being hailed as the silver bullet in the fight against identify theft; however, there are external factors at play that may prevent this from happening. This study investigates if the following five factors, identified from a review of privacy and technology acceptance literature, have an influence on the potential adoption of online biometrics by the internet user community:- perceived security concern, perceived privacy concern, social influence, perceived ease of use and perceived usefulness. Additionally, it sets out to identify, as selected by the survey respondents, the best online biometric trait (Fingerprints) and best biometric security solution (biometric and pin combination). It also identifies whether or not the respondents are concerned about identify theft of which 90.4% said they were.

Seven hypotheses were formulated and each one tested using statistical analysis. In addition, a mixed-method approach using an online survey was targeted at the internet user community to collect quantitative and qualitative data for further analysis. The qualitative data being used to support findings. This study found that five of the hypotheses were supported with the three constructs perceived security concern, perceived privacy concern and social influence having a direct impact on the potential adoption of online biometrics. The findings suggest that respondents were willing to adopt and use online biometrics. Of interest is that higher security and privacy concerns specific to biometrics led to stronger potential adoption of online biometrics. So it would seem that for those surveyed, the benefit of this technology outweighs the security and privacy risks associated with it.

Table of Contents

List of Tables and Diagrams

Tables

Diagrams

Abbreviations

ATB	Attitude Towards Behaviour
ANOVA	Analysis of Variance
BTP	Biometric Technology Product
FMR	False Match Rate
FNMR	False Non-Match Rate
ITRC	Identity Theft Resource Centre
OECD	Organisations for Economic Co-operation and Development
PBC	Perceived Behavioural Control
PEOU	Perceived Ease of Use
PU	Perceived Usefulness
PPS	Personal Public Service
TRA	Theory of Reasoned Action
TAM	Technology Acceptance Model
SD	Standard Deviation
SN	Subjective Norm

1. Introduction

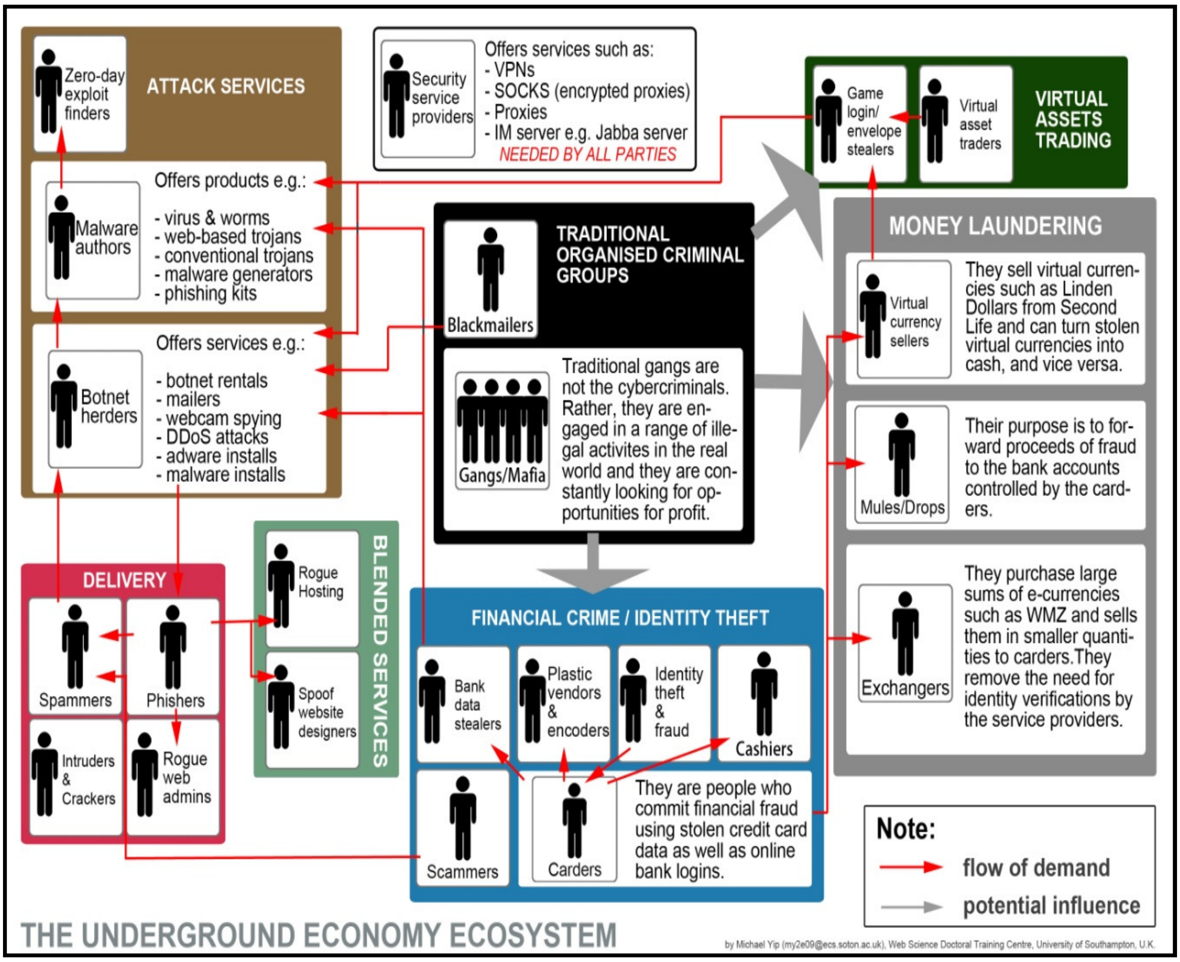
1. 1 Context

From its humble beginnings in the seventies, no one could have foreseen that the internet would become such a critical communications system; it has evolved into a single infrastructure where telecommunications, social media, publishing and commerce converge. Having access to this phenomenon has in general had a positive impact on society; it has revolutionised how we do business, the dissemination of information and how we work and interact. Technological advancements, such as broadband and the smartphone, have played a key role in this. The internet is now readily accessible to those who want it, which has facilitated an increase in e-commerce transactions and has also led to the phenomenal growth of social media websites, such as Facebook & Twitter where individuals regularly post personal details about themselves and their friends.

However the Internet does have an unsavoury element to it. Online criminality is flourishing with an estimated one million victims of cybercrime worldwide on any given day (European commission, 2012a). Cybercrime is a broad term used to describe any crime that is perpetrated through the use of the internet or via other communication technologies. It is normally associated with the following crimes: - online identity theft, computer fraud, illegal pornography and hacking of computer systems. Everyday it has been estimated that up to 600,000 Facebook accounts are blocked as a result of hacking attempts (European commission, 2012b). Policing the internet is proving difficult and the search is on to find the silver bullet. One such technology is online biometrics security systems, the purpose of which is to prevent identities being stolen which can have devastating effects on the victim in terms of the aftermath associated with fraud e.g. impacted credit ratings. The objective of this dissertation is to identity factors that may have an impact on end users/the internet user community potential adoption of this technology to prevent identity theft.

1.2 Identity Theft

In recent years, banking Institutions and government agencies have begun to move their consumer facing business online to reduce costs. Before these services can be used individuals are requested to register their personal information online, e.g. PPS number and home address, for verification purposes to validate that they are indeed who they claim to be. So by default, ‘Identity’ seems to have become the ‘new money’ (Corsby, 2008). This coupled with the success of social media sites, has unfortunately led to a more sinister development; traditional criminal gangs, looking at ways to increase their revenue, have begun to exploit the easy access to personal and financial information online by using the services of cybercriminals. Online identity theft has grown into a thriving billion dollar black market economy where in the US alone, a recent study estimated that $21 billion was stolen in 2012 and there was an increase of one million consumers affected by identity theft fraud when compared to from 2011 figures (Javelinstrategy, 2013). The criminal network is highly organised and the schematic overview presented in Figure 1.1 details just how complex it can be. There are a number of actors involved in the process; traditional gangs can exert an influence on Identity theft cybercriminals to do their bidding, which comprise of e.g. Carders who commit financial fraud and engage with those involved in money laundering to conceal the source of ill-gotten gains or there are scammers who involve the delivery services of spammers and phishers to direct attacks. They in turn can engage with botnet herders and malware authors to develop solutions that can be used to get access to personal information and assist in stealing identities.



Traditional gangs are not the cybercriminals. Rather, they are engaged in a range of illegal activites in the real world and they are constantly looking for opportunities for profit.

They sell virtual currencies such as Linden Dollars from Second Life and can turn stolen virtual currencies into cash, and vice versa.

Their purpose is to forward proceeds of fraud to the bank accounts controlled by the carders.

They purchase large sums of e-currencies such as WMZ and sells them in smaller quantities to carders.They remove the need for identity verifications by the service providers.

They are people who commit financial fraud using stolen credit card data as well as online bank logins.

FIGURE 1.1 – Cybercriminal Underground Economy Ecosystem (source: http://www.michaelyip.me.uk/projects/posters/poster_royalsoc.pdf [Accessed 12th June 2013)

Low barriers to entry and quick turnaround in generating profits have made Identity theft an attractive undertaking for criminals. Moreover, it has given rise to side mini-industries where criminals, not content with setting up their own 'Fraud' factories for mass Identity theft sprees, are also coaching other criminals in how to carry out similar crimes (Dunn, 2012a). The tools required to commit an identity theft can be easily purchased, botnets can be hired for as little as $255 and website hosting for a phishing scam can be obtained for as little as $10 (Bram, 2013), third party cookies can be created and activated to track online activities and store personal information. Ingenious malware such as the trojan horse 'Zeus' have been created to infect any device and can steal sensitive login details to online banking sites. In the summer of 2012, attacks with ZEUS bypassed the two factor authentication security mechanisms employed by banks and was responsible for 36 million euros stolen from 30 thousand bank accounts (Rahid, 2013). The more common online Identity thefts are recognised as being (Wolff, 2007):-

- **New Account creation:**

  Personal information illegally obtained from internet sites is put to use to set up new lines of credit. Bank accounts and credit cards can be opened in an individual's name unbeknownst to them which could result in bad credit ratings, individuals being contacted for unpaid debt and the emotional stress that comes with being wrongfully accused.

- **Account takeover:**

  Another favourite, is account takeover. This can be devastating to an individual, their bank account can be emptied within hours, and multiple purchases made on debit cards / credit cards; it may take a period of time before it is corrected. Essentially, individuals are duped into passing on their personal data including passwords to the guilty party – the methods commonly used are phishing and pharming.

- **Phishing:**

  Unsolicited but legitimate emails are sent to targeted individuals directing them to phony or cloned sites to gather their personal and financial information. The websites may offer goods or services which can be purchased once registered – this is a double whammy, as the goods or services purchased do not materialise and financial and personal information is also stolen. In another form of phishing, the mail requests the individual to renew a subscription with an accompanying threat that if they don't they will lose their protection or invalidate their guarantee. Another method, which is becoming less common, is an unsolicited email from the perpetrator that suggests that the target is entitled to a large sum of money, however personal and bank information is requested before monies are transferred.

- **Pharming:**

  This is a more evolved form of phishing, the main difference is that it is not targeted at individuals, rather it done is en masse via email or on the server side e.g. using the email delivery system. On opening an infected email attachment, the victim inadvertently activates logic which comprises the system host files. The malicious program then converts urls in the background and when the victim types in the correct web address they are redirected to a cloned site. This can also be done on the server side en masse with the same effect, redirecting individuals to copy websites.

In a virtual world without boundaries, stolen information such as identities are a fast selling commodity – and in many cases passed on to a third party by the initial perpetrator for a fee (See Figure 1.1) e.g. "Credit card details can be sold between organised crime groups for as little as €1 per card, a counterfeited physical credit card for around €140 and bank credentials for as little as €60." (Doyle, 2012). So it is very possible that in a short period of time, information such as credit card details could be illegally used across many countries before the damage is known.

Besides financial crimes using stolen identities, there are other equally devastating crimes that can be committed. One example being medical identity theft which involves stealing identities to obtain costly medical treatments. This can result in long lasting effects for the victim such as an altered medical history which could be difficult to remove from his/her medical file and huge medical bills.

1.3 Online Security and the Future

With the media reporting on identity theft, people are becoming aware of the dangers associated with this crime and the potential damaging consequences which were mentioned earlier. In response, trust, security and verification are becoming important elements when transacting online. Online security technology is evolving but websites have been slow to change. Currently there are three types of authentication:

- **Single factor authentication:-**

  Of the three, this is the most recognised and one most utilised by online websites. It requires a user login ID and password. On registering with some sites, the strength of password is checked using an algorithm and the individual is given an indication of the password strength – some sites require a minimum level before they will allow registration to complete. One of the realisations with this type of authentication is that it can be easily compromised if websites are successfully hacked or indeed key-logger malware installed on the persons machine. Another problem is that people are suffering from password overload and in many cases resort to using the same password or variation of the password for the multiple sites they have affiliations with (MacLeod, 2005).

- **Two factor authentication:-**

  Is a step up in terms of security, it is slowly being rolled out - Google and Facebook have offered it since 2011 and both Microsoft and Twitter are now using it (Paul, 2013). This form of authentication requires two pieces of information which are normally a password and a fob that generates a pre-determined pin code, this makes it more difficult for a hacker to compromise an account. However, the problem with this authentication is that it still requires the memorisation of a password and the user also needs to take the fob with them – which takes the convenience out of the whole online experience especially when there is a move toward internet on the go. Moreover, while it may deter cybercriminals for a while who will focus on easier targets, they will adapt and this seems to be already happening, with the successful attack on an airport VPN reported in 2012 using a citadel Trojan to grab the vpn login details and the one time password presented (Dunn, 2012b)

- **Third factor authentication:-**

  Further technological advancement has led to another type of authentication which is now been advocated and is being hailed as a potential silver bullet to combat cybercrime (Kleist,V.,2007). This authentication is known as biometrics and the advantage it has over traditional methods, is that it increases security and convenience. It is the only form of authentication that uses an individual's biological data to identify that they are who they say they are.

1.4 Research Question

As cybercriminals are becoming more sophisticated in their approach to stealing identities (e.g. phishing and pharming methods), the internet user community must become more vigilant to protect their personal data online. Current single-factor and two-factor authentication systems have already been compromised by criminals (see section 1.3). Third factor authentication using online biometric technology may be the technology to prevent Identity theft. However, with any new technology there may be factors at play that prevent its adoption. This purpose of this dissertation is to identify these factors. With that in mind, the research question is as follows:

Identify the key factors that will influence the potential to adopt and use online biometrics and also to examine:

- Is identity theft a real concern for online community?
- Which biometric technology is the best fit for online use by the user community?
- Will the online community feel secure with just biometric verification alone?

1.5 Value of Research

This research aims to examine the factors that affect the adoption of online biometric security by consumers online; with the internet being more accessible there has been an increase in e-commerce activity and unfortunately online fraud. Currently, to date, there has been little research on the adoption of online biometric security for online point of sale purchases. Therefore, there is a need to research the customers' intention to use this technology which would also benefit companies which are looking to secure point of sale transactions online and minimise the risk of fraud.

The research model used in this study is an extended version of the Technology Acceptance Model. The Technology Acceptance Model which includes the perceived ease of use and perceived usefulness constructs is extended to include the following constructs, a security construct (security concern), a privacy construct (privacy concern) and a construct from the unified theory acceptance model (social influence).

1.6 Dissertation Target Audience

This dissertation should be of interest to technology firms which have or are planning to have a biometric footprint. The research is also of interest to the general public. No matter how great a technology, it will be consigned to the scrap heap if the target market does not buy into the offering; the target market in this case being the internet user community and companies with an online presence.

The benefits of this research are two-fold, it will inform the general public about biometrics and how can it be used to prevent identify theft. In addition, technology firms will be informed of public concerns concerning the technology which they can then address before they develop and market their product.

1.7 Scope of this Dissertation

This dissertation will investigate the factors which play a role in determining whether or not the public will adopt and use online biometric tools as a means of verification. The study will also look closely at security and privacy behaviour patterns of the internet user community; it will garner their opinions on the inherent value of biometric technologies and determine whether or not they are ready for the implementation of verification biometric tools.

1.8 Dissertation Roadmap

This dissertation comprises five chapters which are structured as follows:-

Chapter 1

So that the research findings are not taken out of context, this chapter provides the underlying basis of the research. It gives an insight into how prevalent Identify theft is, the impacts and the fact that it is now a multi-million euro industry in the black economy. It highlights the main authentication mechanisms used to combat this crime, introduces online biometric verification systems, the research questions and the target audience of this dissertation.

Chapter 2

Is a literature review of the relevant literature that pertains to the research question. As it is a relatively new area, there is not a lot of academic research completed in the area of interest. The literature review has been broken down into sections. A critique was undertaken of the following:- identity theft, current biometric literature and biometric systems, behaviour and technology acceptance models which have been used in the past and present to study the adoption of new technologies and finally internet privacy models. In the final section of this chapter, a new conceptual model is proposed which combines a number of different constructs and presents a framework to address the research question.

Chapter 3

This chapter centres on the various methodologies that are in use today when conducting research, the research methodologies were analysed and the most suitable one was selected for this research. The reasoning behind the selection for this research is discussed.

Chapter 4

In this chapter the results from the online survey are documented and the findings are analysed and discussed.

Chapter 5

The final chapter presents a discussion of the findings – bringing the dissertation to a close. It outlines the conclusions and also highlights areas which may merit additional research, refinement and development.

2. Literature Review

2.1 Introduction

While the implementation of online biometrics is still in its infancy (Tassabehji and Kamala, 2012), the last decade has seen biometrics become an established discipline. Much research has been completed in the area of its practicality and suitability; yet, there is limited research examining and identifying the factors which may have an impact on its use and adoption online.

Given that the purpose of this dissertation is to add to the existing body of knowledge, it was key to identify a repeatable approach that would examine whether or not the specified factors affect the adoption of online biometrics. A review of the existing literature was undertaken to identify whether existing technology acceptance, behaviour, privacy models could be used; with none being found a proposed model was put forward to confirm if the identified factors; Security, Privacy and Social influence have an impact. Moreover, a review of the existing Identity theft and biometric literature was undertaken to define identify theft and a biometric system which would suit online implementation.

2.2 Identity Related Crime

Identity related crime is an umbrella term that refers to a number of different types of crime, such as Identity fabrication, Identity manipulation and Identity theft, each of which centres around the misuse or creation of identities to facilitate criminal activity (Smith, 2010). As Identity Theft (hereafter referred to as ID theft) is still a relatively young research field, the academic research literature pertaining to it is poor (Fujun *et al.*, 2012) with some limited studies conducted into behavioural aspects (Milne and Bahl, 2004). One of the first countries to recognise online identity theft as a crime was the USA after it was noticed that a high incidence of identity fraud coincided with the emergence and popularity of the internet (Saunders and Zucker, 1999). There are many definitions of Identity theft, one of more reputable from the Organisation for Economic Co-operation and Development (OCED) which defines it as:

'*ID Theft occurs when a party acquires transfers, possesses or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes'* (OCED, 2008, pg. 3).

According to the Identity Theft Resource Centre (ITRC), ID Theft can be subdivided into four main categories, three of which concern individuals (see Table 2.1). The fourth is related to business identity theft where accounts are opened fraudulently in the name of a business to acquire loans or merchandise. (Ramaswamy, 2006).

TABLE 2.1 – Types of ID Theft

Type of ID Theft	Description
Financial ID Theft	Take over an individual's account or take out a loan in their name
Criminal ID Theft:	Uses an individual identity for the purpose of committing crimes
ID cloning	Individuals details are used in daily life for set up of utility bills etc.

As there is now a focus on ID Theft due to the high levels of fraud committed, there has been a renewed focus in the area of biometrics and it application as a security offering.

2.3 Biometrics

2.3.1 Beginnings

Contrary to popular belief, biometrics is not a new tool in the fight against identify theft. According to the literature, it origins can be traced as far back as 6000 BC, where the recording of physical traits was used for identification purposes, e.g. height was used as a distinguishing biometric in the time of the Pharaohs (Davies, 1994). The term biometrics itself comes from ancient Greek words Bios (life) and Metron (to measure) (Maguire, 2009) and it recognises that no two people are the same; there is always a distinguishing characteristic, whether it be a physical or a behavioural trait.

For a trait to be considered, it must be measurable and satisfy the following criteria: (Jain and Ross, 2008).

• Universality-	All persons should have the characteristic
• Uniqueness-	No two people should have the same characteristic
• Permanence-	It should not change over time
• Collectability-	the characteristic can be measured quantitatively

Being the only form of authentication that directly authenticates an individual (Jain, 2004), the risk of fraud and identify theft is said to be minimised (Ahmed and Siyal, 2005). Biometrics offer recognised advantages over the more traditional authentication methods.

It offers increased security, is not easily compromised and is difficult to manipulate by 'stealing, forging, sharing or destroying' when compared to password/token traditional systems (Gokulkumari and Lakshmi, 2011). It is also more convenient as passwords do not need to be memorised or security tokens/fobs do not need to be with a person when access is required.

Biometrics is becoming more widely accepted as the answer to online fraud (Fischer, 2007). As it minimises the potential risk for online fraud, it is an attractive option for governments who are currently leading its diffusion into the public domain. Where this technology is applied, there are three steps that need to occur before a person is granted access to a system:

- **Enrolment**:

  User must enrol in the service and agree for their digitalised information to be stored for future use. Information is digitalised using an appropriate scanner – e.g. Fingerprint scanner. The data is compressed and stored in database for retrieval at later stage.

- **Compression/Evaluation:**

  When trying to gain access to an online account, the user data presented will be compared against previously stored data.

- **Presentation:**

  This is where the results are processed and returned

Over the years research and advancement in this area has focused on a number of key measurable human attributes that can be used to identify individuals apart. These have been segregated into two groups:- Physical and Behavioural; the former being the most accurate and the latter the less expensive of the two (Ngugi *et al,* 2011). While these technologies have been applied to some degree already, e.g. biometric passports, the online application has been slow to take off due to a number of challenges that have to be surmounted first (Ngugi *et al,* 2011). These range from accuracy of the results of the biometric identification systems to non-technical challenges such as user privacy, trust, non-acceptance and security concerns (James *et al*, 2006).

2.3.2 Biometric Systems

For biometrics to be established as one of the key players in the fight against identify theft, a unique identifier must be identified and serve as an input into a system for storage where it can be used in the future for validation purposes. These systems comprise a number of integrated components (Modi, 2011) to form a pattern recognition engine. The sub-systems are listed as follows:

1. Acquisition	captures raw biometric data
2. Signal Processing	extracts features from the sample for reference
3. Data storage	stores the feature template
4. Matching	compares two features to produce a similarity score
5. Decision Making	takes similarity score and matches it to a threshold

A biometric system is used to capture this information and can be split into either one of two different groupings based on a basic fundamental distinction – the method it uses to authenticate an individual. Two authentication methods are widely used today, Identification and Verification. - (Bolle *et al,* 2004, Nanvanti *et al,*2002).

- **Identification authentication method:**

  Recognised as offering a pure biometric authentication, it is solely based on body measurements (Bolle *et al*, 2004). A 1: N approach is used to compare the presented data against the complete set of records in the database to establish the individuals identity (Nanavati *et al,* 2002).

- **Verification authentication method**:

  A different approach is used with this method; it is concerned with confirming whether or not individuals are who they claim to be (Gokulkumari and Lakshmi, 2011). Using a 1:1 approach, it relies on a combination of biometric data and unique identifiers to identify which record should be selected to compare and match against the input data.

Of the two, verification methods are not considered a pure Biometric identification system (Bolle *et al* 2004) as they cannot identify who an individual is based on analysis of digitalised data alone. They work on the principle that the individuals tell the system who they are, the system then verifies this and returns a Yes / No verdict. Conversely, Identification systems are a more complicated system whose purpose is to return an Identity (Gokulkumari and Lakshmi, 2011). Of the two, the identification system is the more complicated system, its goal is to return an identity, this requires extensive search capabilities across the database resulting in more complicated systems that are more difficult to implement than verification systems (Bolle *et al, 2004*). Another downside of the identification system, when compared to verification systems, is a reduced level of accuracy due to extensive matching that needs to be performed to establish an identity which can in turn lead to an increased risk for error (Nanavati *et al*, 2002). An example where a biometric identification system would be used is in a law enforcement agency where fingerprint data would be checked against all records in a database to ensure that the individual is who they say they are to get admittance to a secure area or to apprehend criminals where a 100% match is required. Checks such as this are labour intensive and impact performance. Conversely, biometric verification systems is where digitalised data submitted is compared against a previous stored record containing the persons data, if both match the persons gains access . This process is a lot faster than an identification system. An example of potential applications online would be authentication for banking or other e-commerce sites.

2.3.4 Best Biometric Characteristic

As usability, accuracy and performance are key factors in ensuring continued online traffic to websites, verification systems are the most appropriate for online transactions in the consumer space; they are faster and more accurate than identification systems (Gokulkumari and Lakshmi, 2011). To identify the best biometric characteristic it must have these five qualities (Wayman, J.1999, Wayman J 2001)

TABLE 2.2 – Five Qualities that a Biometric characteristic should have

Quality	Definition
Robustness	Must be a feature that is not susceptible to any change over time
Distinctiveness	Has to be distinctive and show great variation such that no two people will have the exact same characteristic
Availability	Everyone should have the feature in multiples so at least it has the potential to be compared against all individuals
Accessibility	Is easy to capture image using capture devices such as electronic sensors
Acceptability	There is no objection to have the measure taken for enrolment

While the literature does not necessarily identify the best biometric characteristic per se, research has gone onto the selection of the best biometric technology to use. According to

Reid,(2003)**,** there are a number of factors that need to be taken into consideration when selecting the best biometric technology to use:

- Users must be willing to accept it.
- Users must find it easy to use
- Technology is reliable and mature
- Technology requires the user to be actively involved
- Technology has lower false acceptance rate
- Technology has highest possible false rejection rate
- It is small in size and requires little space
- Users become habituated quickly to the device.
- Technology costs are such that there is a return on investment
- Technology is deployable and supportable

There are many types of Biometrics which can be split into the two categories, Physical and Behavioural (Modi, 2011):

Physical:-	Fingerprints, Face, Iris, Hand geometry, Vascular pattern, Retina
Behavioural:-	Voice, Dynamic signature, Keystroke dynamics

Using these factors, Reid (2003) conducted research to determine which of the following biometric types: - voice, face, iris and fingerprint, was the most usable technology currently. Fingerprint technology was proven to be the most popular. Not only is it the most widely known in the public domain, it is the oldest and most mature biometric technology. This finding is also supported by a case study carried out by, Tassabehji and Kamala, 2012, they applied the system usability scale (Brooke, 1986) to evaluate, from a user perspective, the effectiveness of a biometric authentication system for online banking. With a sample size of 116 people, they concluded that a biometric systems would be looked on favourably with over 67% of respondents investing time to get their biometric data recorded for the initial set up of the verification system, but also that biometric fingerprint technology was considered to be the most suitable of all the biometric technologies followed by Iris technology and facial recognition.

As noted by Obaidat & Boudriga 2007, traits are not without their disadvantages, some of the advantages and disadvantages are listed in table 2.3.

TABLE 2.3 – Advantages and Disadvantages of Key Biometric Traits

Biometric Trait	Advantages	Disadvantages
Fingerprint	• De-facto standard for identification • Easy to use • Mature technology • Advance recognition systems	• Quality may vary • Fingerprints can be damaged
Facial Recognition	• Universal trait • Technology already inbuilt in many internet ready devices	• Poor accuracy • Wireless use increases difficulty for imaging • High false negative rate in bad light
Iris Scan	• Iris pattern is unique and stable • High level of accuracy	• High cost • High quality imaging conditions required

2.3.5 Biometric Weakness

Unfortunately, while being more secure than password authentication systems, biometric security systems are not 100% fool proof. The systems work on a threshold value system due to the potential of background noise. An inherent weakness of this approach is that it does allow for false positives and false negatives which could shake peoples belief in the system. A false positive is where a person is accepted as another individual and gains illegal access while a false negative is where an individual is refused access as they are incorrectly identified as another individual.

- False positive:

Otherwise known as the False Match Rate (FMR) – this determines how easy it is for an imposter to match the threshold level after a number of attempts - (Wayman and Mansfield, 2002)

$$\text{FMR} = \frac{Number\ of\ imposter\ comparisons}{Total\ number\ of\ imposter\ comparisons}$$

- False negative:

Also known as the False Non-match Rate (FNMR). (Wayman and Mansfield, 2002). Converse to FMR, individuals are wrongly identified as not being who they say they are and as a consequence are not granted access.

$$\text{FMNR} = \frac{Number\ of\ rejected\ genuine\ comparisons}{Total\ number\ of\ genunie\ comparisons}$$

If either of these ratios is high, the system will not be suitable for verification purposes. The technologies are by no means fool-proof, using physical artefacts researchers have been successful in bypassing biometric security systems. Matsumoto *et al* 2002, wrote a report on how to a successfully spoof fingerprint biometric systems using gelatine based materials. In another study, facial recognition systems were simply fooled by presenting a high resolution photograph of the person that was been impersonated (Thalheim, L, *et al,* 2002). Even with Iris recognition systems, a physical characteristic that is so unique that the two eyes of the same individual are different was spoofed using cosmetic contact lenses.

However, as noted by Modi, 2011 there are anti-spoofing measures in place to counter this; but as technology advances, attacks will become more innovative. Developers will need to take into account the vulnerabilities and to assure the public of the viability of biometric technologies and design appropriate solutions without impacting performance. Moreover, implementers of the systems will have to ensure that proper security controls are in place. As biometric verification authentication systems are a relatively new technology in terms of online application, understanding the factors that may aid or adversely impacts its adoption is critical for its success.

The aim of this research is to examine the factors affecting the potential adoption of online biometrics. This involves examining various users perceptions that have been previously identified as impacting the intent to transact and intent to use new technology systems. To identify the relevant factors for online biometric testing, the following sections will focus on internet privacy concern models and technology acceptance models to identify constructs appropriate for this dissertation.

2.4 Privacy Concerns

A major concern of privacy advocates is that biometrics can violate the privacy of an individual (Modi, 2011), an individual is bound to his or her physical or behavioural trait and once digitalised the biometric 'password' is permanently assigned. The data is stored in a database, however one can never be sure that it is entirely safe from theft and unlike passwords which can be changed, if your information is compromised, it is not possible or a least it is very difficult to change your biometric data. Even though this is true, research has been completed in this area and a viable solution to the storage of biometric data, is biometric encryption (Khalil-Hani *et al*, 2013.)How it works is as follows, the biometric information is taken to create a biometric encryption key – once created the biometric data is discarded. In order to gain access to the system in the future, the users' biometric data is used to unlock the encryption.

With the phenomenal growth of the internet, the 9/11 terrorist attack and social media networking the concept of privacy has evolved and is now a top concern for individuals and other stakeholders such as business leaders and government regulators (Smith *et al*, 2011). Privacy itself has many definitions, first and foremost in the legal sense – it is the right to be left alone (Warren & Brandeis, 1890, as cited in Pavlou 2011). A subset of this, is information privacy which in the context of information technology age and recent advances in technology and social media, researchers refer to the rights of an individual in controlling how their data is collected and used (Mason,1986 & O'Neil, 2001). This also includes personal communication privacy and data privacy (Bélanger & Crossier, 2011).

A number of studies have been conducted in relation to privacy concerns which have resulted in the creation of privacy scales; one of the first was the creation of the CFIP scale (concern for information privacy) which was used to measure an individual's concern about organizational privacy practices (Smith *et al*, 1996). It is a fifteen point scale reflecting four dimensions of privacy concern (see Table 2.4).

TABLE 2.4- Four Dimensions of Privacy Concern for CFIP

Dimensions	Description
Collection	Concern with amount of personal data collected
Errors	Concern that protections against deliberate and accidental mistakes are inadequate
Secondary use	concern that information collected is used for another purpose
Unauthorised access to information	concern that information is ready available to people that should not have access

In an empirical study completed by Stewart and Segars (2002) the validity of this scale was confirmed. However, this model was created for offline activities and is not suitable for the internet application where users could differ in their concerns about privacy online versus offline. To meet this need, it was subsequently enhanced giving rise to the IUIPC - Internet users information privacy concerns model (Malhotra *et al,* 2004). In contrast to the CFIP, this is a ten point scale categorised in the following three elements which are more attuned to the internet space.

TABLE 2.5- Three Dimensions of Privacy Concern for IUIPC Model

Factors	Description
Collection	Concern with amount of personal data collected relative to the benefit value received
Control	Freedom to exit at any time
Awareness	Understanding condition, practises and how information is used

The IUIPC model more accurately reflects what happens online and is also supported by findings from Dinev and Hart (2006).They note that an individual's perception of what happens with the information they provide online is represented by the level of their privacy concern. Moreover, additional research has been conducted to measure privacy concerns and determine their impact on internet usage. Investigating the trade-offs between privacy concerns and internet use, it was concluded that privacy concerns have an impact on the decisions of users to conduct business over the internet (Dinev & Hart, 2003). But, as noted by Buchanan *et al* (2007), in a paper which was based on existing research exploring relationships between values and interests in the context of privacy concerns (Introna & Pouloudi, 1999), privacy concern is subjective.

Dinev and Hart expanded on this research and went on to identify two antecedents which play a salient role in determining privacy concern and the intent to transact, these are internet literacy and social awareness (Dinev & Hart, 2005). They proposed a theoretical model to test their hypothesis.

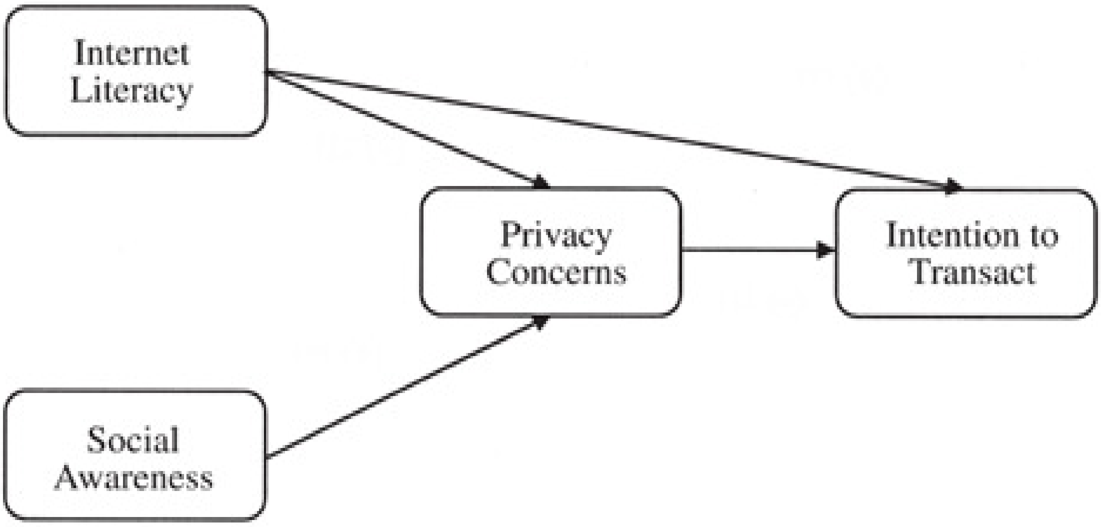


FIGURE 2.1 – Privacy Concerns Model Reproduced from Dinev & Hart 2005

From their study, they concluded that internet literacy had a negative impact on privacy concern and a positive impact on intention to transact while social awareness has a more positive affect on privacy concern. In their study, the definition of internet literacy was taken to mean the ability to use a computer which is connected to the internet to accomplish practical tasks. Social awareness was defined as being interested and knowledgeable about initiatives as well as polices with relation to technology and internet. Privacy concern may also impact the willingness of individuals to be profiled (Van Slyke et al. 2006).

A study by Keng Lin *et al*, (2010) undertaken in Malaysia, found that perceived risk associated with an individual's personal privacy and security online had an influence on the adoption of biometrics in online applications. A more recent study (Ngugi *et al*, 2011) found that perceived security had an influence on perceived trust of a system which in turn influenced intention to use biometric technology. As enrolment of personal digitalised data is a prerequisite for using online biometric systems, perceived privacy and security concerns specific to the technology could impact its adoption. In terms of the potential adoption of online biometrics, no one study reviewed has examined both of these factors separately to determine their individual influences on intention to use or adopt biometric systems.

As this study is looking at the potential adoption of this technology by the internet user community who may consider both privacy and security as a concern, both of these factors will be looked at separately in this study. However, on reviewing the literature, these two factors alone are not used to measure adoption of new technologies, section 2.5 looks at acceptance models which were found to be generally used for this purpose.

2.5 Acceptance Models

On reviewing the existing IS&T and social psychology literature, conceptual models have been defined which try to capture accurately an individual's intention to perform an action. These models are rooted in the field of social psychology and have been applied universally. Models which are commonly used in the field of information systems usage adoption research are:-

- Theory of Reasoned Action (Fishbein and Ajzen,1975)
- Theory of Planned Behaviour (Ajzen, 1985)
- Technology Acceptance Model (Davis, 1989)
- United Theory of Technology Acceptance (Venkatesh *et al*, 2003)

Before these models were conceptualised, research in the field of Social Psychology at the time focussed on the constructs attitude and behaviour, however it suffered from a lack of clarity and direction which led to varying results in research performed (Fishbien and Ajzen, 1972). Aiming to bring direction and focus to this research field, a conceptual model was formulated by Ajzen and Fishbein (1975).This became known as the Theory of Reasoned Action (TRA) which not only allowed the integration of other theoretical approaches to 'Attitude' but also a presented a means to predict behaviour intention (Fishbein & Ajzen, 1975) see Figure 2.2.

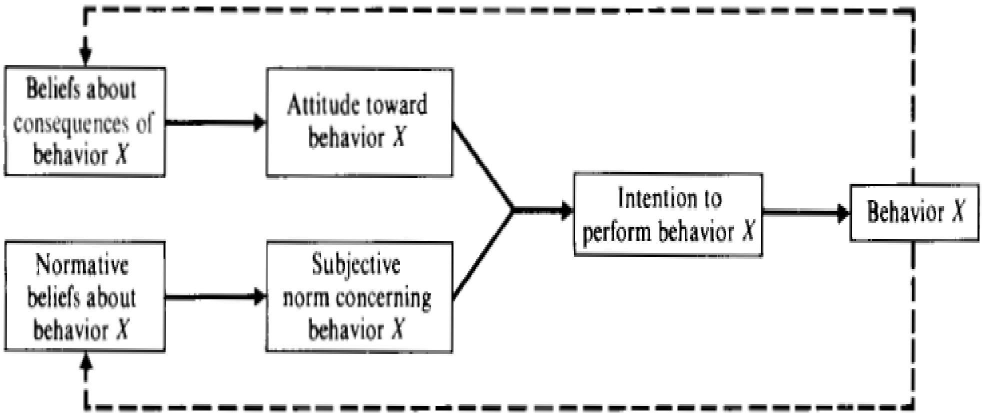

Beliefs about consequences of behavior X
Attitude toward behavior X
Intention to perform behavior X
Behavior X
Normative beliefs about behavior X
Subjective norm concerning behavior X

FIGURE 2.2 Theory of Reason Action (source: Fishbein & Ajzen, 1975)

The TRA model hypothesises that an individual's behaviour intention (BI) is jointly determined by two constructs, the individual's attitude towards performing the behaviour (ATB) and the individual's perception of what significant others think they should do which is known as subjective norm (SN). Depending on the scenario, one is more dominant than the other in predicting BI – where an individual may be performing an action on behalf of someone else SN is the more dominant if it is for the individual alone, ATB is more dominant with SN having little relevance (Ajzen and Fishbein, 1980). In a meta-analysis of past research using the TRA model, Sheppard et al (1998) concluded that it did have a strong predictive utility even for scenarios it was not originally intended for; the model has been applied with success in many empirical investigations across a number of disciplines (Sheppard *et al,* 1998). However, in the same study, Sheppard noted that it is not always suitable as there are three limiting conditions due to the generality of the model.

Table 2.6 – Limitations of TRA Model

Limiting Factor	Impact
Goal versus Behaviours	• Not suitable for goal intentions as does not take into account how goals are determined – influences of probability of failure or consequences of it. • Does not take into consideration non-volitional controls
Choice among alternatives	• TRA focuses on determinants of a single behaviour • Presence of choice may change the nature of intention and the model does not account for this
Intention versus Estimates	• Does not take into account that intention to use is different from what one might expect to do if there are external factors that could lead to an unsuccessful attempt

With respect to the limitation concerning the influence of non-volitional factors, Azjen extended the model to include another construct called perceived behavioural control (PBC) to make it more robust and measure these factors. The updated model became known as the Theory of Planned Behaviour (Figure 2.3) and with this added component; he postulated that it would be able to predict actual behaviour and behaviour intention (Azjen, 1985).

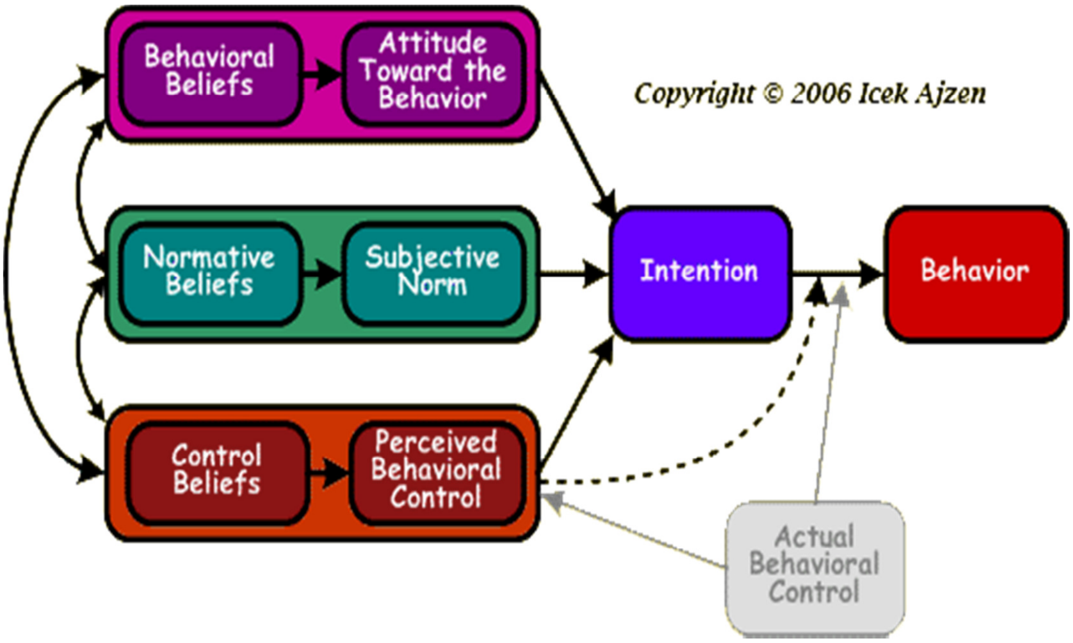

Behavioral Beliefs
Attitude Toward the Behavior
Copyright © 2006 Icek Ajzen
Normative Beliefs
Subjective Norm
Intention
Behavior
Control Beliefs
Perceived Behavioral Control
Actual Behavioral Control

FIGURE 2.3. – Theory of Planned Behaviour

The additional construct –, 'perceived behavioural control' refers to an individual's perception of their ability to carry out a particular behaviour. Later, it was surmised that this construct is affected by the sum of control beliefs multiplied by the perceived power of the control factor over the belief (Ajzen, 1991). The construct 'Intention' is influenced by the outcomes of the three antecedent constructs of 'attitude', 'subjective norm' and 'perceived behaviour' which as reflected in Figure 2.3 have a direct impact on the measurement of intention to use. So for example, where there is favourable ATB or SN, if the individual does not believe that they have control over performing the behaviour for whatever reason e.g. confidence/time/resource constraints, it is possible they won't intend to use it.

The versatility of the TPB model is that it can be applied to all research fields where there is a need to measure an individual's intent. Nevertheless, while this model has become popular in measuring behavioural intention, it does suffer from a weakness in that it does not account for perceived difficulty which would have a stronger influence on prediction of intentions and behaviour than perceived controllability (Azjen, 2001).Both of these models can be used to measure usage of a technology in the context of information technology, however these models don't take into consideration one key element, 'ease of use', this an element which has become increasingly important in the area of IT, especially as individuals become more familiar with online technologies.

One model that does examine this is the Technology acceptance model (TAM) which was conceptualised by Davis in 1986 and is widely used in the IS/IT literature for predicting the adoption and acceptance of technology. It is an extension of the TRA model and is tailored to the modelling of user acceptance of information systems (Davis *et al*, 1989). Its' purpose is to explain the determinants of technology acceptance in a meaningful generic way which is capable of explaining user behaviour across end-user IS technologies, yet staying within the boundaries of the TAM model (Davis *et al*, 1989). The model introduces two new constructs, 'perceived usefulness' (PU) and 'perceived ease of use' (PEOU); both of which are useful in the determination of an individual's intention to use a technology. These constructs can either positively or negatively impact the users attitude towards a technology and by default their intention to use. It has been posited that these two constructs are two of the most important determinants of system usage and intention to use (Wu and Wang, 2005). The constructs measure the following:

- PU captures how the technology benefits an individual's performance,
- PEOU captures an individual's understanding of the effort to use the technology.

While the TAM model is similar to the TRA and TRB model in that it postulates that usage is determined by BI, where it differs is that BI is jointly determined by attitude towards using the system and PU (Davis *et al*, 1989) .TAM does not take into account subjective norm.

Behavioural intention = A + U

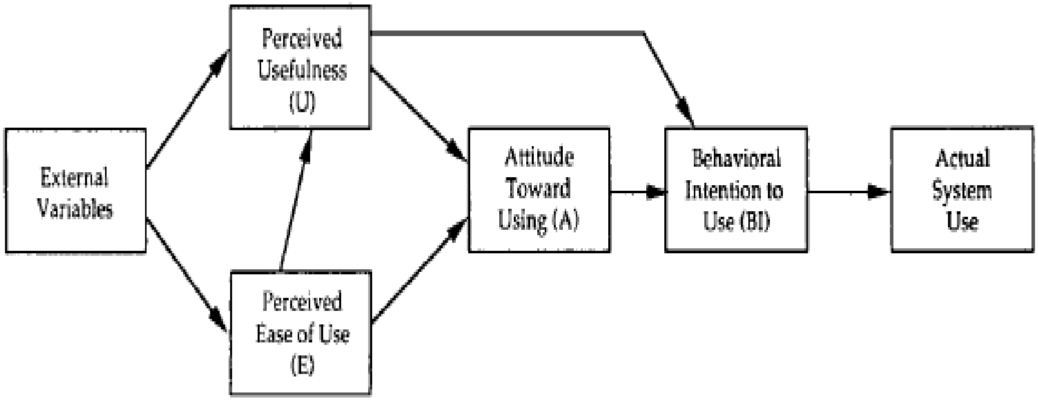

Perceived Usefulness (U)
External Variables
Attitude Toward Using (A)
Behavioral Intention to Use (BI)
Actual System Use
Perceived Ease of Use (E)

FIGURE 2.4 Technology Acceptance model (Davis,1986).source Davis *et al,* (1989)

Even though it is widely used, there are those who are critical of TAM (Bagozzi, 2007) accusing it of being too simple and leaving out elements that do have an impact on behaviour; one such element being emotion (Venkatesh, 2003). Others suggest, based on empirical research, that there is unexplained variance when using the TAM model in similar circumstances which should theoretically yield similar results. They conclude that the TAM model should be updated with additional constructs which will enable the variance to be fully understood across different studies (Legris, 2003).

To help explain this variance, the TAM model underwent a number of transformations; in 2000, Ventakesh and Davis, extended the TAM Model to include social influence and cognitive instrumental factors which they identified as having an influencing impact on the factor of 'perceived usefulness'. These were as follows:-

TABLE 2.7 – TAM2 List of Social Influence and Cognitive Instrumental Factors

Categories	**Factors**
Social Influence	Subjective norm
	Image
Cognitive instrumental	Job relevance
	Output quality
	Result demonstrability
	Perceived ease of use

This extended version of the model is known as TAM2. Each factor plays a role in determining behavioural intent: - two of the constructs, subjective norm and image are said by Ventakesh and Davis to have a positive impact on perceived ease of use. TAM2 posits that perceived ease of use and result demonstrability will have a positive influence on perceived usefulness (Ventakesh and Bala, 2008) while the job relevance and output quality jointly have an impact on same, 'the higher the quality output, the stronger the effect job relevance will have on perceived usefulness' (Ventakesh and Bala, 2008, p. 278).

Furthermore, when investigating low rates of employee adoption of technology in the workplace, Ventakesh and Bala (2008) proposed a new model called TAM3, this model is a combination of the TAM2 model (Ventakesh and Davis, 2000) and the model of the determinant of perceived ease of use (Ventakesh, 2000). The purpose of this model is to help those at managerial level to make decisions on the adoption of technologies. When compared to the other TAM model, TAM3 is the more comprehensive model, not only does it identify factors affecting perceived usefulness and perceived ease of use; it clearly states from a theoretical perspective that determination of perceived usefulness does not influence perceived ease of use (Ventakesh & Bala, 2008). Additionally, it takes into account the moderating effects of experience; it 'posits that with increasing experience, while the effect of perceived ease of use on behavioural intention will diminish, the effect of perceived ease of use on perceived usefulness will increase.' (Ventakesh & Bala, 2008, p. 278).

However, even though the Technology adoption models do seem to be more applicable to IT technology adoption than their predecessors, in a 1995 study another model was proposed, ‘Decomposed Theory of Behaviour’ model as an alternative to the TPB (Todd and Talyor, 1995). It is marketed as being more complete than the TAM models going to a more granular level as it identifies more factors to influence usage such as breaking down the constructs of subjective norm and perceived behavioural control to allow the understanding and capture of other influences such as perceived ability and control that may impinge on intention (Ajzen 1991, Talyor and Todd 1995).

In a study completed by Ventakesh, a review of eight previous models was undertaken and the constructs were consolidated to formulate a unified model. Those eight models were 1) theory of reasoned action,2) theory of planned behaviour, 3) technology acceptance model, 4) motivational model, 5) a combined theory of planned behaviour/technology acceptance model, 6) model of personal computer use, 7) diffusion of innovations theory, and finally social cognitive theory. The model is known as the Unified theory of acceptance and use of technology (UTAUT) which is rooted in the Technology acceptance model. (Ventakesh *et al*, 2003). The Intention of the UTAUT (fig 2.5) model was not only to merge existing models into one but from a business user/ research community perspective to explain how an individual intends to adopt a technology and in addition capture and explain usage behaviour.

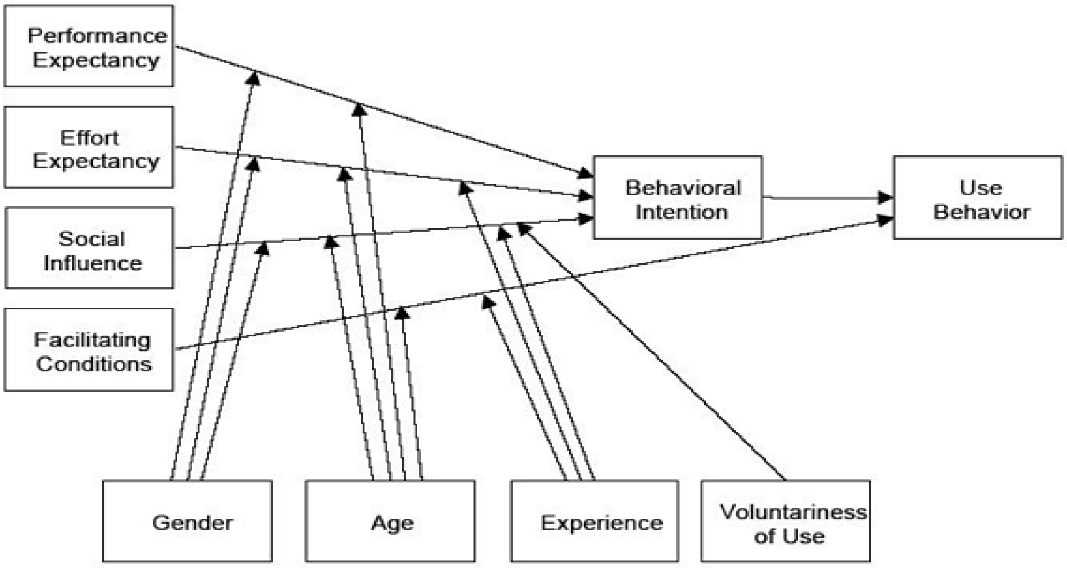


FIGURE 2.5. Unified Theory of User Acceptance Model

As can be seen from Figure 2.5, the conceptual model is comprised of four key constructs:- performance expectancy, effort expectancy, social influence, facilitating conditions which are impacted by the constructs gender, age, experience and voluntariness of use. The key constructs, have a direct impact on behavioural intentions and usage. Ventakesh et al, stipulate that approx. 70% of variance can be explained by the UTAUT model. This would suggest that it is possible to have a complete model with regards to usage behaviour and intention. (Ventakesh and Bala*,* 2008).

In 2007, Bagozzi suggested that the whole field was at the precipice of chaos with all the variations of models. He admitted that even though the UTUAT model is a more comprehensive model than its predecessor, TAM, it is more complicated to apply – so in effect, the selection of the model depends on what needs to be achieved with the study and the timeframe allotted to it.

Online biometrics is a new technology which will potentially be used by the internet user community. From the review of the literature undertaken, technology acceptance models are central to determining if a technology will be used and adopted. Using well established constructs which are universal to all technologies they are good indicators in identifying the influencing factors, such as in the case of the biometric study previously mentioned in section 2.4 which used constructs from the TRA, TPB and TAM models (Keng Lin *et al*, 2010). In reviewing the models, the constructs that were of most relevance to the adoption of online biometric systems were selected. The proposed model is described in the following section.

2.6 Conclusions:

In reviewing the literature, TAM has outperformed both the TRA and TPB models (Davis et all 1989, Venkatesh et al., 2003). In the last 20 years, TAM has been used extensively in empirical investigations and is said to be a better predictor of an individual's intention to use a technology (Agarwal & Karahanna, 2000).

As Biometrics requires the enrolment of personal details, security and privacy may also play a role in the adoption of this technology. From the literature, with the continuous drive to extend the acceptance models, it is clear that they are not all encompassing, none of those reviewed take into consideration that privacy concern and security may play a role in influencing the adoption of online technologies. As the enrolment and storing of an individual's data is integral to the online biometric solution, concerns about privacy and security should play a pivotal role in whether or not the technology will be adopted. The possibility does exist that if individuals are overly concerned they will shy away from using it.

As part of this study, there are a number of hypotheses that require investigation to determine if they have an impact on adoption of online biometrics. The TAM model is not equipped for the number of factors being examined. So the model is extended to include elements of the Privacy scale model and UTAUT model to test the following hypotheses. (Figure 2.6)

H1: PEOU has an impact on adoption of online biometrics

H2: perceived security concern impacts adoption of online biometrics

H3: perceived usefulness will have an impact on adoption of biometrics

H4: perceived privacy concern has an impact on adoption and use of online biometrics

H5: social influence has an impact adoption and use of online biometrics

H6: PEOU has an influence on PU

H7: Privacy concern has an influence on Security concern

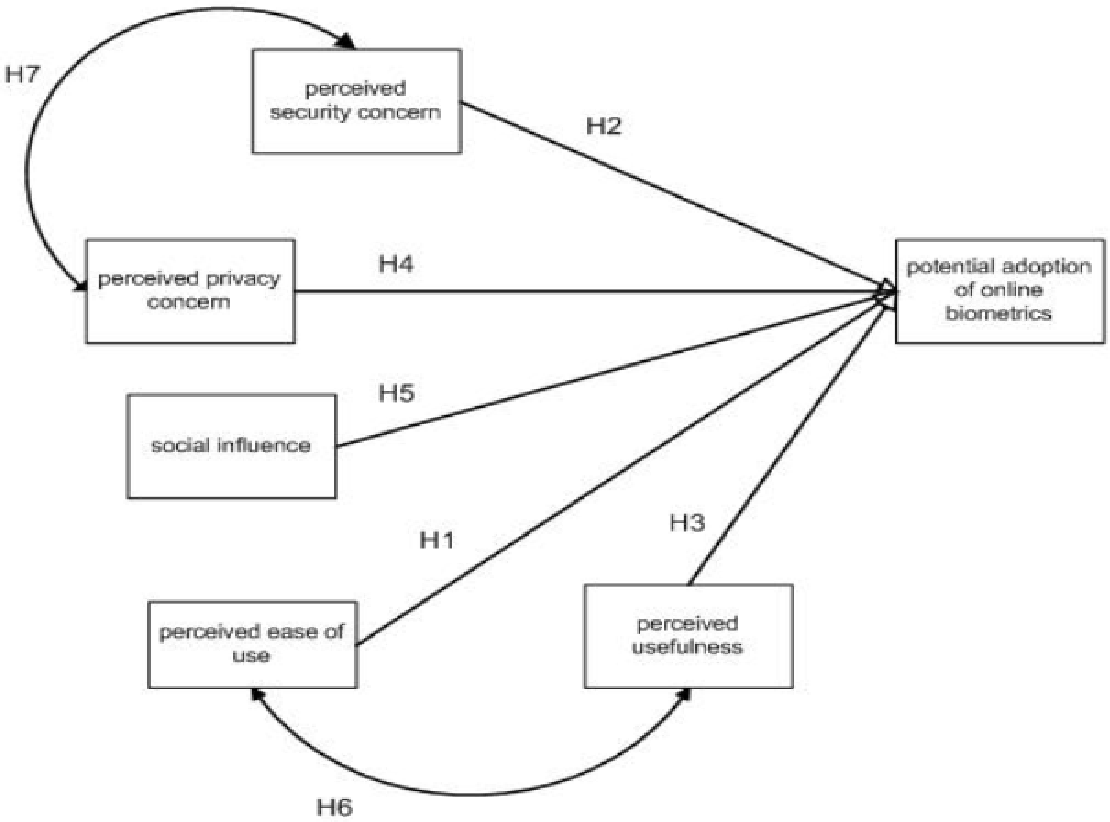

H7
perceived security concern
H2
perceived privacy concern
H4
potential adoption of online biometrics
H5
social influence
H1
H3
perceived ease of use
perceived usefulness
H6

FIGURE 2.6 – Proposed Potential Adoption Model

Using statistical analysis, the null hypothesis for each of the 7 hypotheses will be tested. The null hypotheses states that there will be no effect between the two constructs being measured. Where the null hypothesis is proven false, the alternate hypothesis is supported. Further detail of the statistical analysis can be found in section 3.7 and chapter

4. The approach and steps taken to collect the data and analyse it are discussed further in chapter 3.

3. Research Methodology

3.1 Introduction

Through research, knowledge can be expanded. Data is collected and analysed, questions are answered and other lines of inquiry are found, all adding to the existing body of knowledge. Not all research is successful; it is not enough to focus on certain research methods just because they are current, time must be taken to select the most appropriate research methodology which provides a systematic way of how to answer the question. As noted by Saunders, assumptions inferred by the chosen research philosophy are a decisive factor in choosing the research method and strategy (Saunders *et al*, 2009).

The chosen philosophy for this dissertation is Pragmatism – which can involve both quantitative and qualitative approaches to be undertaken. In this study a mixed method research methodology was selected, as it was best suited to provide more reliable results in the timeframe provided.

3.2 Selection of Methodology

Saunders research onion model was used as a tool to help formulate the research methodology. Consisting of six layers, it provides a framework in which to build the methodology.

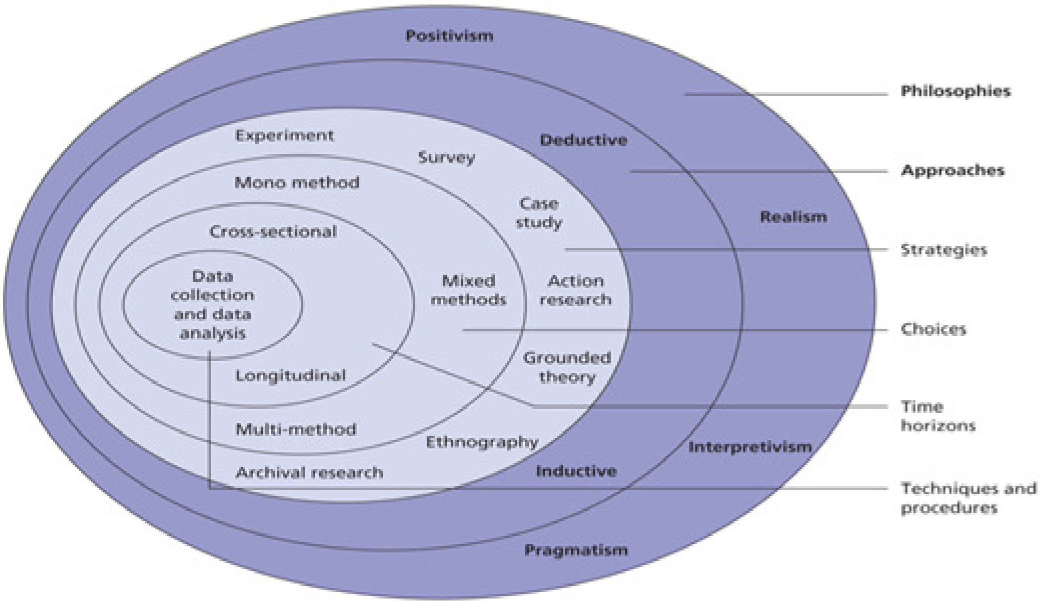


FIGURE 3.1 – Research onion - Reproduced from Saunders *et al* 2009 pg 108. – source Mark Saunders, Philip Lewis and Adrian Thornill.

The first step in selecting the methodology was to understand the research objectives and the direction to be taken.

3.2.1 Research Objectives

The purpose of this study is to identify factors affecting the adoption of biometrics and determine whether the general public are ready for this next phase in identity theft prevention. With this in mind, the study will look to identify the following:

- existing online behaviour with regards to security and privacy
- views on biometrics and intention to use

A cross-sectional group will be targeted to obtain suitable data that will be analysed thoroughly to determine if the data supports the hypotheses in relation to the potential adoption and use of online biometrics as presented in the proposed model in section 2.6. Qualitative data will also be reviewed to support findings.

3.2.2 Selection of Research Philosophy:

Taking the ontological and epistemological positions of three philosophies:- Positivism, Interpretivism & Pragmatism into consideration, each was examined to gauge their suitability in answering the research question and meeting the objectives of this study.

Of the three, Positivism is closest to the research approach of natural science, only being interested in what can be seen and observed. It is not interested in the subjective opinion of people while maintaining that the researcher should remain objective and completely independent at all time. This unbiased approach can lead to the creation of law like generalisations (Remenyi *et al*, 1998) and is suitable where an existing theory is being used to test a hypothesis. According to Gill and Johnson 2002, a highly structured methodology is used by the researcher and there is also emphasis put on statistical analysis (Saunders *et al,* 2008).

Conversely, Interpretivism advocates a subjective approach, with the emphasis being on the people rather than objects. Also the researcher is not independent and is expected to understand the social interactions between the people in the environment being studied; data is collected from subjective meaning and social phenomena (Saunders *et al,* 2009) using qualitative methods. This philosophy is ideal for discerning peoples' views on new technologies which is one of the objectives of this study.

Choosing Positivism over Interpretivism or vice-versa is limiting in the direction the research should take. On the other hand, the Pragmatist approach focuses on answering the research questions using elements from both philosophies. As noted by Saunders *et al*, (2009) the mixed method approach provides the best possible answer to the research questions. It uses a combination of quantitative and qualitative methods to collect and analyse the data. The philosophy allows pragmatists to use both objective and subjective viewpoints when analysing the data providing greater insights. For that reason, Pragmatism was selected for this study, using the interpretivist approach it will allow opinion to be formed on the future of biometrics verification, while the positivist approach will quantitatively analyse data to prove or disprove the hypotheses

3.2.3 Selection of Research Approach

There are two research approaches: - deduction and induction. Deduction is aligned more to the positivist approach, it is mainly used where a theory is developed and the research strategy is designed to test the hypothesis; Induction on the other hand, is aligned to interprevist approach, this is where data is collected and analysed to formulate a hypothesis.

Of the two, the deductive approach is a lower risk strategy as it is quicker to complete while the inductive approach can be slower and it is possible that no pattern emerges (Saunders *et al*, 2009) As there are both positivist and interpretivist approaches in the research question, elements of both will be included, however the main focus will be on the deductive approach. Qualitative data will be used to lend support to the data and address any gaps that may arise in the quantitative findings.

3.2.4 Selection of Research Strategy

A number of research strategies were reviewed to see if they could provide a suitable means of collecting the data:-

- The ethnography approach was dismissed on the grounds that it is too time consuming as the ‘researcher needs to immerse herself or himself in the social world being researched as completely as possible’ (Saunders *et al*, pg. 149, 2009) and it is deeply embedded in the inductive approach.

- Archival research was not considered as it requires the analysis of administrative records as the principal source of data, (Saunders *et al*, 2009)

- The case study approach, even though it can be very thorough was not suitable as no organisation was identified on which a case study could be conducted and if there was, it would be impossible to generalise the findings unless an embedded case study approach was taken which is more time consuming.

- Action research was not viable, it is more suitable to research within an organisation and the researcher himself or herself is part of the organisation being studied which is not the intention of this study.

- Grounded theory on the other hand was a strong contender, while mainly associated with the inductive approach, it does in fact allow for both inductive and deductive approaches to be used (Saunders *et al,* 2009). However, Suddaby (2006) suggests that it is not a straight forward approach and requires considerable experience to be well executed. Moreover, it is used in theory building rather than hypothesis testing which is the objective of this study

Of the strategies reviewed, a survey was deemed the most suitable. It is mainly associated with deductive research (Saunders *et al, 2009*) but can also support exploratory qualitative research as well. As the main rationale of this research is deductive and the target segment is the online community, it prompted two decisions from the beginning. The first decision being the survey design should take the form of a formal standardised questionnaire with prescribed answers lending itself to quantitative and statistical analysis to test the hypotheses. In addition, to get the opinions of target audience, a small number of qualitative open ended questions were added to the survey to get public perceptions on biometric technology. The second decision was to put the survey online availing of the online survey services in operation, e.g. SurveryMonkey.

Online surveys have many advantages over other types of research strategy; they allow for both quantitative and qualitative research to be conducted and have been proven to be:

- Less time consuming and more cost–effective than mail surveys/ focus groups (Roztocki, 2001).
- Far-reaching (Evans and Mathur, 2005).
- Allow for a wide range of questions to be asked and information collected (Ilieva *et al,.* 2002).
- Convenient for data collection and analysis (Evans and Mathur, 2005).

Moreover, it was felt that those with access to email would be competent with computer technology and would not have any difficulty with accessing the online survey or executing it. Also as the survey was online, it was possible to check response rates and save backups of the data in case the online system got corrupted and data was lost.

Survey length is seen as one contributory factor to low response rates (Deutskens *et al,* 2004). With this in mind, the survey was structured and designed as follows:

- Divided into sections; Suitability, Biometrics, Security, Privacy & Demographics
- Questions were optional
- Where possible likert type items were grouped to reduce the number of questions
- Explanations were provided where required (highlighted by pilot survey)
- Allow for Quantitative and Qualitative data to be collected at same time (Parallel data gathering, see section 3.2.5)

An online third party application, surveymonkey will be used to publish the survey online. The advantage of surverymonkey is that the data can be collected and displayed in graph format allowing for a quick initial interpretation. Also raw data can be downloaded in a format required for statistical packages such as SPSS. Moreover by placing the survey online, it is cost effective allowing for a larger group of participants to be targeted at no extra cost.

3.2.5 Selection of Research Method Choices

Of the two research choices available, the multiple method approach was selected as it is not limiting like the mono-method (where a single data collection technique is used and the corresponding analysis procedures, e.g. questionnaire and quantitative analysis). The multiple method approach has been advocated by many (Curran and Blackburn 2001, Tashakkori and Teddlie, 2003) as the belief is that quantitative and qualitative methods/procedures cannot be separated when doing research.

Multiple methods are further sub-divided into four groups: - multi-method quantitative, multi-method qualitative, mixed method research & mixed mode research. Of these four sub-groups, the mixed method research using the concurrent strategy was selected, it allows for both quantitative and qualitative data to be collected simultaneously, such as a questionnaire with both closed and open ended questions (Jupp, 2006). The advantage delivered, is that combining the two gives a better understanding of the research question which in turn allows for more detailed analysis and a more complete outcome.

3.2.6 Selection of Time Horizon

Due to time constraints, a cross-sectional snapshot view will be taken rather a longitudinal approach. For the longitudinal approach to be of benefit in this area, it would have to occur over a number of years until online biometrics security becomes mainstream.

3.2.7 Data Collection Method Selection

Using the mixed method approach, as mentioned in section 3.2.4, parallel data gathering was used to collect both quantitative and qualitative data for this dissertation. The advantage is that a broader range of data can be collected that would not normally be possible with quantitative data surveys alone. The online survey consisted of 39 questions with prescribed answers ranging from those with a likert scale to a simple Yes/No answer. It also contained 3 open-ended questions to capture qualitative data that could possibly explain any anomalies in the findings or highlight other possible areas of interest concerning biometric/security and privacy.

3.3 Limitation of Methodology

While using an online web-based survey does have its advantages, there are limitations with this approach which can have an impact on the quantity & quality of data collected for analysis, these include:-

- No scope for extensive discussion as there is with the focus group/interview process
- The questions are the entire scope of what can be asked
- Participants cannot seek further clarification on questions which they may not understand
- The survey may not be well designed and answer the research question
- As a result data collected may be of lower quality over other survey methods
- The survey is self-administered so respondents can opt out of answering questions
- Online survey response rates tend to have a lower response rate than other methods approx. 11% lower (Losar *et al,* 2008)

Some of the limitations mentioned above, such as further discussions with participants could be addressed with in-depth interviews or focus groups strategy. However, taking into consideration the timeframe and costs associated with those approaches and that they are purely qualitative in nature, it was felt that the questionnaire would deliver more and catch a wider audience.

The following actions were taken to mitigate some of these limitations, as specified in section 3.2.4 and 3.2.5, parallel data gathering was used to collect qualitative data as well as quantitative data, the open-ended questions allowing the participant to answer as they so wish. In addition, a pilot survey was first sent out to get feedback on the questions asked and identify any improvements required before it was sent out en masse. Finally, the online survey was sent to a large audience to ensure that the target sample of 100 was achieved.

3.4 Ethics Committee

Before data collection could begin, ethics approval had to be sought; the purpose of which was to ensure that the welfare and rights of those being surveyed was protected. This process involved creating the survey online and sending it to the School of Computer Science and Statistics Ethics committee; it was accompanied with a pdf version of the survey and supporting documentation. On review, no ethical issues were identified and approval was granted.

To adhere to the best practice approach in terms of ethics, the targeted audience were sent background information on the research itself as well as an information sheet detailing the survey procedure and what would happen with the results. This was to insure they were well informed before they partook in the survey and that there was clearly no plan to deceive. Moreover, the participant was given the option of deciding whether to participate or not in the study and if they did, they understood and accepted the declarations.

Ethics approval, including the participant information sheet is in Appendix A.

3.5 Piloting the Questionnaire

Before distributing the questionnaire, the survey was piloted to five colleagues to get their feedback. In general it was positive; all agreed that the questionnaire was interesting. However, some well place comments were heeded to– two of my colleagues felt that the questionnaire had too many questions, though they did admit, that they were able to complete it in ten minutes. One colleague identified a few spelling mistakes which were promptly corrected, while another colleague felt that some of the questions could be arranged differently so as to have likert scale instead of a yes/no option. One colleague found that two questions were duplicated.

All suggestions were examined carefully. Six questions including the duplicates which all related to security were removed, spelling mistakes were corrected and two questions were converted into a likert scale.

The questionnaire was re-issued once more to the pilot respondents to get their final feedback – all felt that the study was more focused and was ready to be sent out. Questionnaire is attached in Appendix B.

3.6 Sample Framing & Sample Size

As the research question was targeting the online user community, the sampling frame was anyone that purchased goods or services online in the last six months and who are working in Ireland. Four age groups were targeted, 21-29, 30-39 & 40-49, 50-59 to gauge their view on adoption of biometrics and on which generalisations could be made. These particular age groups were chosen as it was felt that they were representative of differing levels of online buying patterns across the generations.

For this study a sample size of 100 was deemed appropriate, once achieved the study was to remain open for a further two weeks to get additional responses which could be included in the qualitative aspect of this study.

3.7 Scale Measures

In the survey a number of questions used five point bipolar scales to measure positive and negative agreement to a statement. An example of a five point scale being:

(1) Strongly agree
(2) Agree
(3) Neutral
(4) Disagree
(5) Strongly Disagree

For statistical analysis, the data was recoded in SPSS to allow for analysis where the median could be calculated for likert type items and the mean could be calculated on likert scales (two or more grouped likert type items). This also allowed for additional tests to be performed to examine relationships between factors and the potential adoption of online biometrics. The data was analysed using linear regression, ANOVA testing and Pearson's chi-square analysis (see Chapter 4 for further detail).

3.8 Issuing the Survey

The medium used to reach the target audience was email using both personal email and also work email to target work colleagues. Before the survey was sent to work colleagues, approval was sought and granted from the HR department and the programme manager. (See Appendix C).

The email contained a link to the online survey, a brief introduction to the research and an attachment detailing the background and purpose of the study as well as what would happen to the collected data once the survey was closed down.

Also participants were made aware that they were under no obligation to complete the survey

3.9 Closing Down the Survey

The online survey was closed after 6 weeks. Data was extracted from SurveyMonkey in a format that was suitable for upload into a statistical package for further analysis, SPSS being the software chosen.

Additionally, In accordance with the Data Protection Act 2003, Data collected would be deleted once there was no further need for it.

4. Research Findings and Analysis

4.1 Introduction

In this section, the objective is to test the hypotheses concerning the adoption of biometrics and answer the questions as specified in section 1.4. After closing the online survey, the responses were extracted for subsequent detailed analysis in excel and the SPSS statistical package version 20. Overall the response was high at 80%, which accounted for 127 respondents agreeing to submit the data they provided for further analysis and inclusion in the findings. Initial analysis indicated that 98.5% of considered respondents answered all quantitative questions, while 71% responded to the qualitative questions providing a rich source of data to support findings or understand unexpected outcomes.

Due to the small percentage of respondents not answering some of the quantitative questions, in SPSS a missed category was assigned to those questions and missed responses were excluded from further analysis. 'Don't knows' were also excluded from the analysis. In the analysis phase, where there are two or more likert type items, the items were combined to create a likert scale (e.g. q15 in Appendix b) otherwise they were treated as single items (e.g. q3 in Appendix b). Where a 5 point scale was used, it was collapsed into 3 point scale in some cases to assist with the statistical analysis and to improve the interpretation of results.

Concerning the constructs, Cronbach's alpha was used to examine scale reliability for each construct that consisted of a likert scale. Moreover, to examine the relationship between likert type and likert scale constructs, Levene's test and Anova were used to test the hypotheses. Going one step further a simple linear regression method was used to predict the influencing power the constructs have on the potential adoption of online biometrics. Analysis of the data and the findings will be discussed in the following subsections, each of which will deal with certain aspects of the results. The subsections are organised as follows:

- Suitability & Demographics
- Adoption of Biometrics
- Current online behaviours concerning Security, Privacy and Identify theft

4.2 Suitability and Demographics

The web-based survey was distributed to work colleagues and friends representing a broad cross-sectional age-group of people in Ireland. To determine suitability of the sample, questions related to internet purchases and demographics were asked.

4.2.1 Internet Purchasing Presence

As outlined in the sample frame, to be eligible and considered representative of the target group for this study, the respondents must have purchased items online within the last six months. Those outside of this time period were not considered, as due to their infrequent online purchases they would never see the benefit of adopting and using the online technology. The following questions were asked to determine suitability:

Have you purchased goods or services online in the last 6 months?

One respondent failed to answer this question; of those that did, 98.4% were deemed suitable. The remaining 1.6%, which corresponded to 2 respondents, were excluded from further analysis as they had not purchased items in the last 6 months.

Have often do you purchase online?

Online purchasing habits fell into the following categories (Figure 4.1); the majority of respondents (54.4%) purchased online monthly, followed by the 'less often' category (27.2%) and weekly category (18.4%). No one surveyed purchased daily.

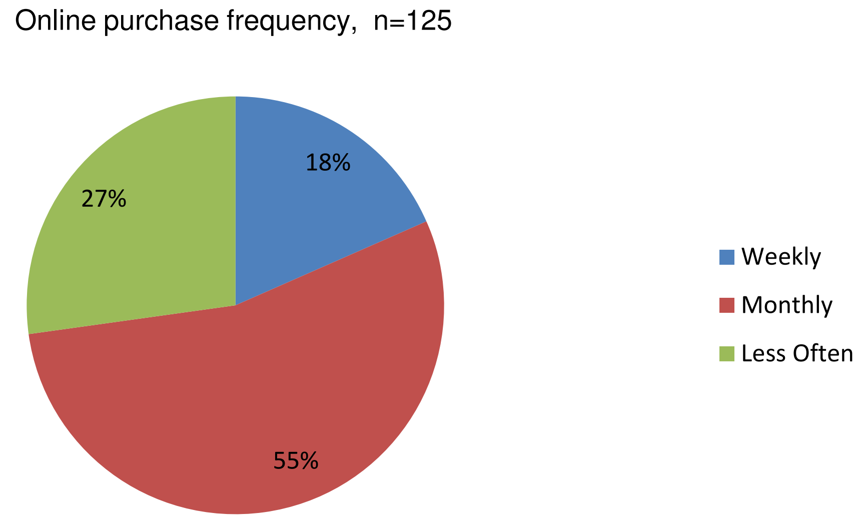


FIGURE 4.1 – Purchasing Online Behaviour

The individual, who failed to respond to the first question, did answer monthly and so was not excluded from the study. In total, data from 125 respondents was considered eligible for further analysis.

4.2.2 Gender & Age group

Participants were also asked the following gender and age group related questions.

What is your gender?

Of the 125 submissions, two failed to enter their gender and so are not represented (Figure 4.2). There was strong representation from both groups making it possible to do further analysis to identity potential differences influenced by gender. The breakdown was as follows:

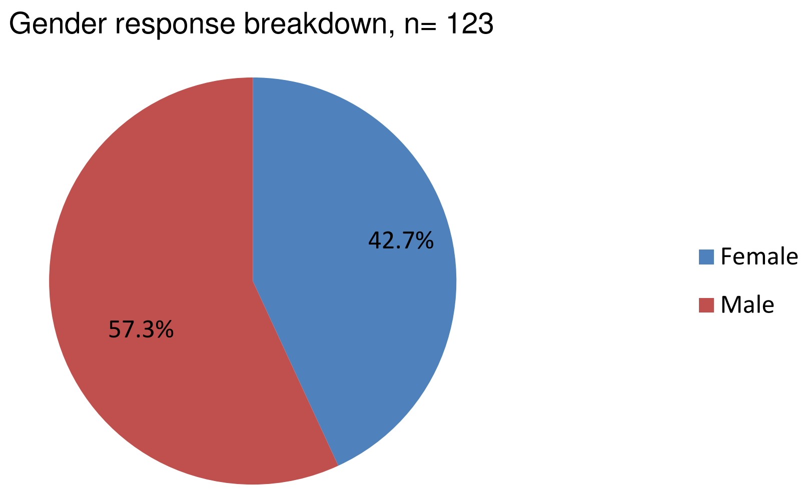


FIGURE 4.2 – Breakdown of Male/Female Response

The higher male response at 56.9% may be due to the fact that greater percentages of males were contacted via work.

Age Category

Which category below includes your age?

One respondent failed to answer this question and there was no response from the 'over 60' or 'less than 20' age category so it was not possible to assess these age groups. The response rate for the 50-59 age category was disappointing with only 2 participants. For further analysis, it was decided to collapse this age group and merge it with the 40-49 category which was renamed to '40 and over'.

As is evident from Table 4.1, there is an unequal distribution across the groups; over half of the respondents (57.3%) are in the 30-39 category. Followed by, the 21-29 and 'over 40' category at 25% and 17.7% respectively. Using cross-tabulation, the male/female gender was captured for each age category (Table 4.1).

TABLE 4.1 - Age Category by Gender, n=124

Age Category	% Breakdown	Male	Female	Response Count
21-29	25.0%	19	12	31
30-39	57.3%	36	35	71
40 and over	17.7%	15	6	22

4.3 Prior Knowledge and Adoption of Online Biometrics

The purpose of the following questions was to identity if prior knowledge of online biometric systems had an impact on the adoption of biometric technology. Of those surveyed, 38.7% did not have any knowledge about online biometrics systems while 61.3% had knowledge ranging from a basic to a good level as displayed in Figure 4.3. No one had expert level.

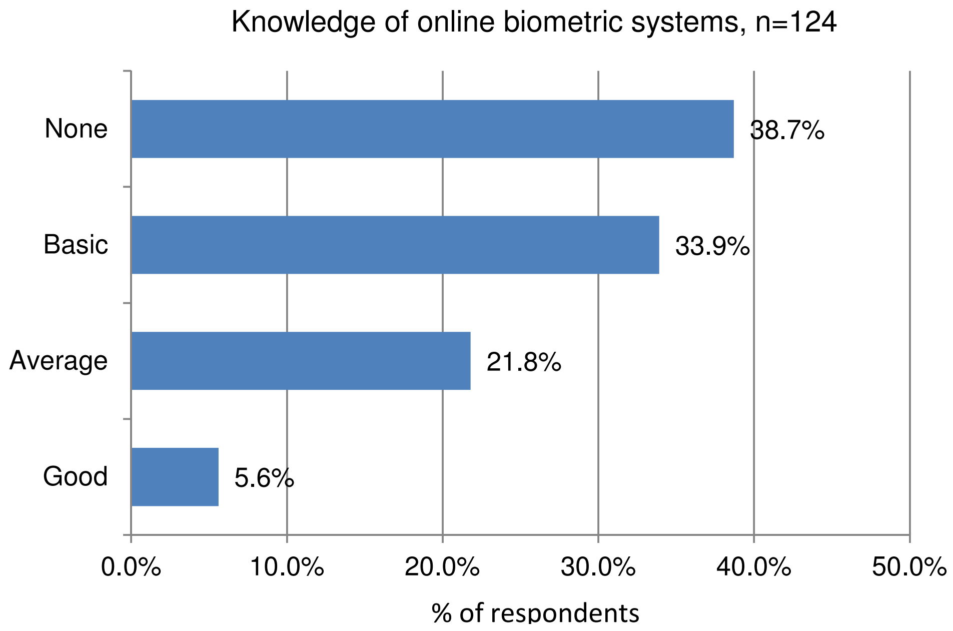


FIGURE 4.3 – Knowledge of Online Biometric Systems

The respondents were asked to grade the technologies from 1 to 5, with 1 being the most favoured and 5 the least favoured. Of the technologies currently being mooted as possible candidates for online biometric use, fingerprint biometric technology was identified as the most usable, followed by iris and facial recognition respectively; it is also interesting to note that the behavioural biometric characteristics were the least favourite. This can be observed from Figure 4.4, where rank of preference uses a sliding scale from 0 to 4 (where 0 is the most favoured and 4 is the least favoured).

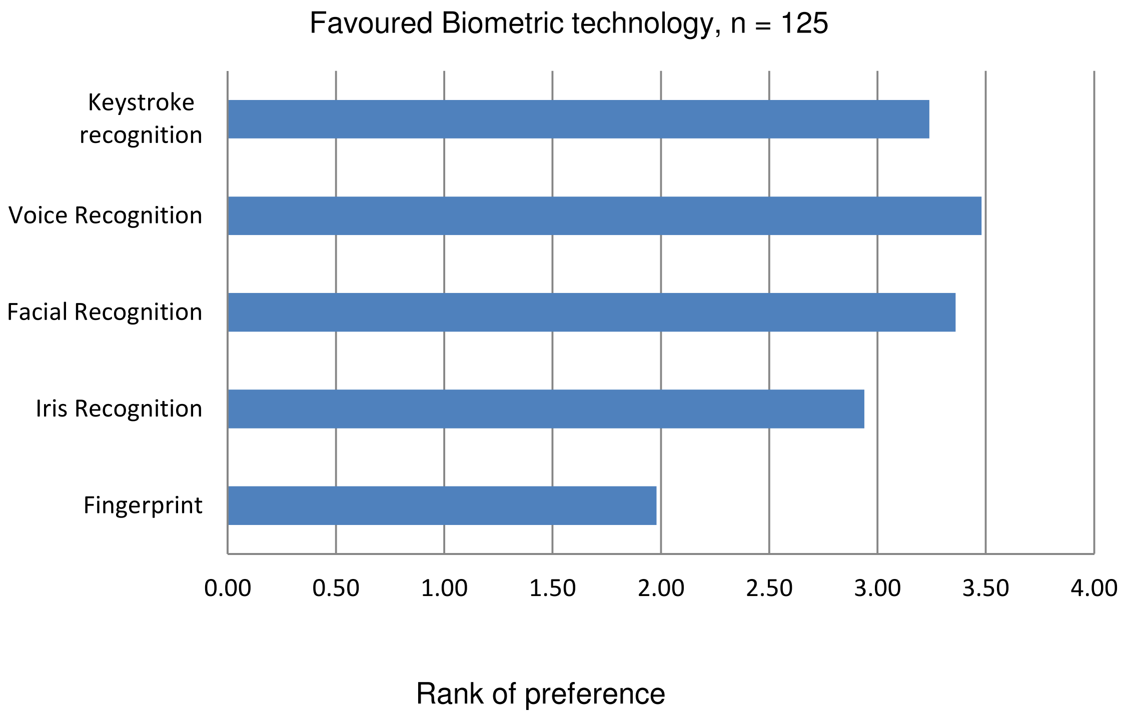


FIGURE 4.4 – Favoured Online Biometric Technology

Even though online biometrics is still in its infancy, the findings observed in Figure 4.3 & Figure 4.4 suggests that the internet user community are indeed aware that biometrics is being fronted as the next wave in security improvements for online activity. However, while there is certainly an interest in it, there are factors that may impact the adoption and use of it which are analysed in the next sections.

4.3.1 Adoption of Online Biometrics Construct

To test the hypotheses raised in this study, see section 2.5, there was a need to measure the potential adoption and use of online biometrics by the respondents. To get this information, the following question and statements were presented in the online questionnaire. (Table 4.2).

TABLE 4.2 – Adoption and Use of Online Biometrics

Q	In order for me to use an online biometric security verification, it would require…?	
	S1	Low cost set up for me as an individual
	S2	A biometric reader app to be made available for the smartphone/tablet
	S3	That the verification system has been in use for some time before I submit my digitalised biometric data

A five point likert scale measure, ranging from 'Strongly agree' to 'Strongly Disagree' was used to capture the data for each likert type statement (see Table 4.3). Recoding was done from 1 to 5 in the direction 'Strongly agree' to 'Strongly Disagree' in SPSS (Table 4.3).

TABLE 4.3 – Adoption and Use of Online Biometrics Response Distribution

Statements	Strongly Agree (1)	Agree(2)	Neutral(3)	Disagree(4)	Strongly Disagree(5)
S1	48.8%	37.8%	7.9%	3.1%	2.4%
S2	34.1%	42.9%	16.7%	6.3%	0.0%
S3	37.8%	48.8%	9.4%	3.9%	0.0%

Likert types were grouped and treated as a likert scale (Boone, D., Bonne, H, 2012). The mean (1.8173) was used to calculate the central tendency with a SD of 0.60959 showing the there is a narrow distribution from the mean. Cronbach's alpha (α=.598) suggests that the reliability of the scale and the internal consistency was poor but only slightly under the questionable grading ($0.6 \geq \alpha \leq 0.7$). However, all these likert type items were required. Further analysis showed that the removal or addition of likert items did not lead to significant changes; each permutation was less than $\alpha = 0.6$.

Additionally, cross-tabulation was performed against this construct to identify if gender and age influenced the potential adoption of this technology. It was expected that younger age groups would adopt and use the technology more so than the others. This was not the case, 87 % of the 20-29 category are likely to adopt and use biometrics compared to

82% of the 30-39 category and 90% for the over 40 category. At over 80%, the potential adoption rate is high for each category and is encouraging for the future of this technology. What is also interesting is that the over 40 category had the highest adoption rate.

4.3.2 Hypothesis 1- PEOU has an Impact on Potential Adoption of Online Biometrics

The perceived ease of use construct associated with the TAM models is used to measure the acceptance of new technologies. A number of related statements were asked in the survey to identify if PEOU has any bearing on the potential adoption and use of online biometrics (Table 4.4).

TABLE 4.4 – Perceived Ease of Use Statements

Q	Use of biometrics will require…	
	S1	Low level training needed as my current experience with online purchasing will make the transition easy
	S2	No special knowledge to submit data for online biometric security verification checks
	S3	That the biometric readers are easy to use
	S4	That I understand how the biometric reader interacts with the online biometric security check before I will use it

A five point likert scale measure, ranging from 'Strongly agree' to 'Strongly Disagree' was used to capture the data for each likert type statement. Recoding was done from 1 to 5 in the direction 'Strongly agree' to 'Strongly Disagree' in SPSS (Table 4.5).

TABLE 4.5 PEOU Statements Responses

Statements	Strongly Agree(1)	Agree(2)	Neutral(3)	Disagree(4)	Strongly Disagree(5)
S1 n=125	18.4%	55.2%	16%	9.6%	0.8%
S2 n=125	8.0%	48.8%	25.6%	17.6%	0.0%
S3 n=124	34.7%	43.5%	17.7%	3.2%	0.8%
S4: n=125	17.6%	51.2%	19.2%	12.0%	0.0%

As there are four likert type items, the items were grouped and treated as a likert scale (Boone, D., Bonne, H, 2012) with the combined score used for analysis. In SPSS, an mean score was calculated for each respondent in a new variable column. The mean of this new variable was then calculated to get the overall mean for the PEOU construct and determine the central tendency. It was calculated to be 2.2440 and the standard deviation calculated was relatively small at 0.51863, suggesting that 68% (empirical rule theorem – 1 standard deviation) of the observations are close to the mean. Cronbach's alpha ($\alpha = 0.390$) showed that the internal consistency and reliability of the scale was poor ($\alpha < 0.6$). With such a low rating, different permutations of items were used to see if this rating could be improved but this was not so. Moreover, items were confirmed to have been coded correctly; individually, each measured perceived ease of use. However, with the group mean and central tendency suggesting that 50% agree that ease of use is important, further analysis was completed with the caveat that result may be impacted due to poor scale reliability.

In order to predict the effect that the PEOU construct has on potential adoption of online biometrics and prove the alternate hypothesis (H_1) a simple linear regression, which also includes the ANOVA test, was performed; potential adoption of online biometrics construct being the dependent variable and PEOU the independent. In analysing the fit of the model, the correlation coefficient (R = 0.135) represented a small effect, while the coefficient of determination (R^2 = 0.018) demonstrated that PEOU only accounts for 1.8% of the variance. Furthermore, analysis of variance with ANOVA (f (.836) = 2.274, p = 0.134) indicated that while the model was a good fit ($f \geq 1$), the chances of getting the same result is statistically high (p > 0.5) without any PEOU effect.

In addition, the standardised coefficient (β_1=0.135) indicated that for every one standard deviation change in the PEOU predictor, there will be a slight increase in the adoption of biometrics by 0.135 of its standard deviation (SD = 0.60959). However, as p=0.134 this result was deemed statistically insignificant thus proving the null (H_0) hypothesis which is that PEOU does not have impact the potential adoption of online biometrics and thus not supporting the alternate hypothesis.

4.3.3 Hypothesis 2: Perceived Security Concern Impacts Potential Adoption of Online Biometrics

With 90.4% of respondents expressing a concern about online identify theft (Figure 4.5), the expectation is that the storage of online biometric data would have an effect on adoption and use of online biometric systems.

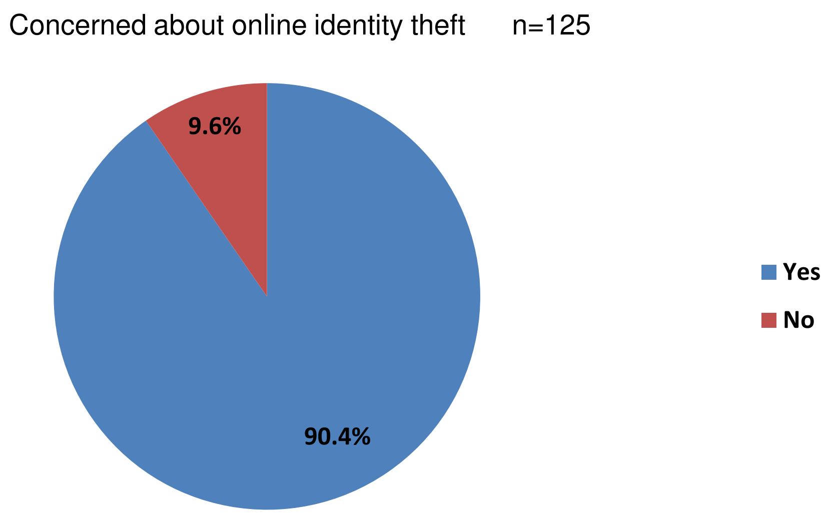


FIGURE 4.5 Identify Theft Concern

The following statements (Table 4.6) were asked in the online survey to capture security concerns that the respondents may have.

TABLE 4.6 – Perceived Security Concern Statements

Q	Storage of digitalised biometric data…?	
	S1	Could be intercepted in transmission and copied for use by criminal gangs
	S2	Security around the storage of biometric data is a concern for me and would prevent me from using online verification websites
	S3	Could be stolen from a company's website and used to impersonate me to commit fraud
	S4	Is not secure enough for my liking, using my biometric data at the time of purchasing to unlock an encrypted code is more secure

Likert type responses in the Table 4.7 were combined to create a likert scale for further analysis. The overall grand mean (2.2907) of the scale was used to determine the central tendency suggesting the 50% of the respondents did have the security concerns. With an SD of 0.71519 demonstrating that 68% of the responses are close to the mean due to a relatively narrow distribution.

TABLE 4.7 Distribution of Responses for Perceived Security Concerns

Statements	Strongly Agree(1)	Agree(2)	Neutral(3)	Disagree(4)	Strongly Disagree (5)
S1 n=125	22.4%	63	20	13	1
S2 n=125	21	32	42	28	2
S3 n=125	42	65	11	6	1
S4: n=124	20	51	33	16	4

Cronbach's alpha ($\alpha = .730$) showed that the internal consistency and reliability of scale was good ($\alpha > .70$). Further analysis was undertaken to determine if security concerns have an impact on the adoption of online biometrics. The simple linear regression method was used to test this alternate hypothesis; the dependent variable was the potential adoption of online biometrics construct and the independent variable the security concern construct. In analysing the fit of the model, the correlation coefficient (R = 0.233) represented a small effect, however this was slightly stronger than the PEOU effect. Also, security concerns account for 5% of the total variance as demonstrated by the coefficient of determination ($R^2 = 0.05$).

Furthermore, analysis of variance with ANOVA (f (2.301) = 6.466, p = 0.012) indicated that the model was a good fit ($f \geq 1$) and the chances of getting the same result without the perceived security concern effect was statistically low ($p < 0.5$). Also, the standardised coefficient (β_1=0.223) which predicts the influencing power, indicated that for every one standard deviation change in the security concern predictor, there will be a slight increase in the adoption of biometrics by 0.223 of its standard deviation (SD = 0.60959). Given that p=0.012, this result was significant statistically thus disproving the null (H_0) hypothesis that perceived security concern that does not have an impact on potential adoption of online biometrics and thus supporting the alternate hypothesis which suggests that it does have an impact.

Also it is important to note that the qualitative data collected further supports this finding. The risk summed up by one individual is as follows, '*Since biometric data is static once intercepted it can be used to impersonate a user for life'*. Of the participants that responded to the following open-ended question: *What factors would prevent you as a user from using online biometrics? (n=91),* 35% of the respondents would not use online biometrics due to concerns with security; these would have to be resolved first.

However, it must be noted that even though security is a concern for the respondents, of those surveyed, 25% admitted to disabling their security settings when surfing online to improve performance (n=125). Of the respondents, 67.7% stated that they had concerns 'Once in a while' when purchasing on line which would prevent them from purchasing items, while 12.4% would purchase items regardless (Figure 4.6).

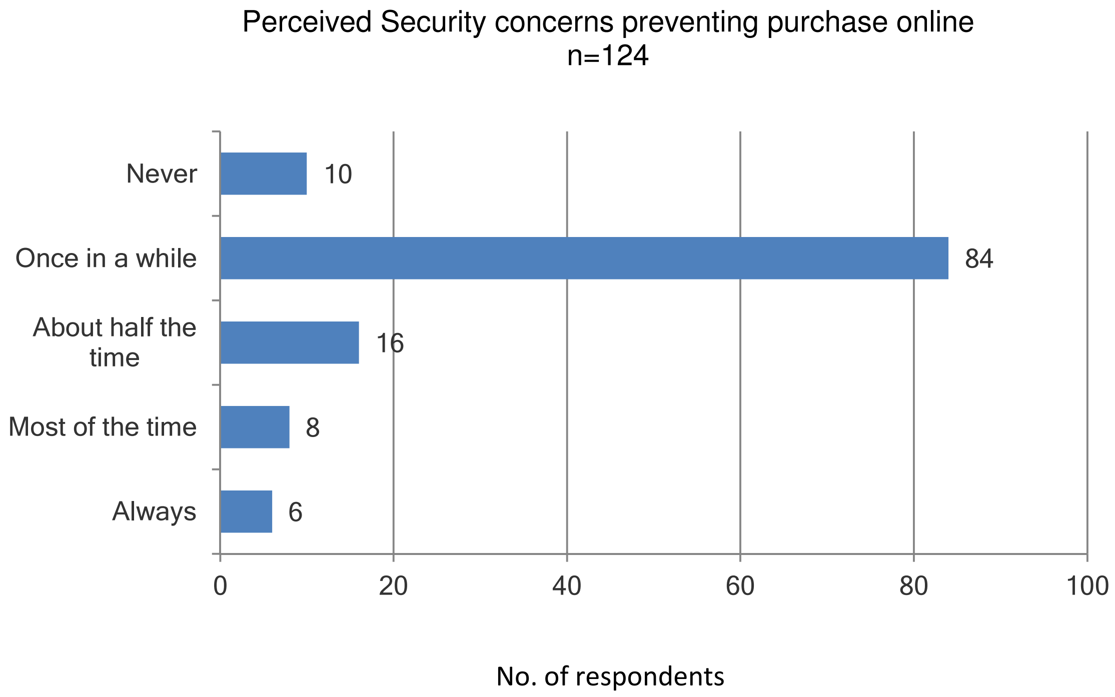


FIGURE 4.6 – Do Perceived Security Concerns Prevent Online Purchasing

The mode was used to calculate the central tendency in this case and as can be observed from Figure 4.6 indicates that the tendency is 'once in a while'. A cross-tabulation between this likert item and the security construct showed that it was not suitable for chi-square analysis (73.3% had counts less than 5 due to the security mean groups). The cross-tabulation showed that 82% of those that answered once in a while agree that security concerns would impact them using online biometrics, yet with the same grouping over 90% would adopt and use the technology given the concerns.

4.3.4 Hypothesis 3: Perceived Usefulness will have an Impact on Potential Adoption of Online biometrics

From the TAM model, perceived usefulness of a technology has also been identified as a factor in technology adoption. As it is a construct in the proposed model used in this study, the following questions were presented in the questionnaire (Table 4.8) for the purpose of obtaining data for analysis.

TABLE 4.8– Perceived Usefulness Statements

Q	The introduction of online biometric verification security systems will	
	S1	Result in further growth in purchases as people will become more confident and secure in using credit card details online
	S2	Make it more difficult for cyber criminals to steal my identity
	S3	Make it near impossible for the imposter to be verified as the individual they are trying to impersonate.
	S4	Always verify me as the real user
	S5	Will be the silver bullet in the fight against online criminal activity

The 'Don't know' category, as it is fundamentally different from the neutral category, was excluded from the analysis. On creating the likert scale, the mean (2.1096) was calculated to determine the central tendency which indicated that 50% agreed that perceived usefulness would entice them to use online biometrics. The SD. was 0.6107 indicating that there was a narrow distribution of responses close to the mean. Cronbach's alpha $(\alpha = 0.870)$ showed that the internal consistency and reliability of scale was good $(\alpha > 0.80)$.

TABLE 4.9 – Perceived Usefulness Responses

Statements	Strongly Agree(1)	Agree(2)	Neutral(3)	Disagree (4)	Strongly Disagree(5)	Don't Know
S1	12.8%	46.4%	26.4%	10.4%	0.8	3.2%
S2	41.6%	51.2%	1.6%	2.4%	0%	3.2%
S3	14.4%	46.4%	25.6%	9.6%	0%	4.0%
S4	6.4%	32%	27.2%	19.2%	7.2%	8%
S5	10.5%	46%	22.6%	13.7%	1.6%	5.6%

As with the PEOU and Security concern constructs, a simple linear regression was performed to predict the effect that PU may have on the potential adoption of online biometrics. In analysing the fit of the model, the correlation coefficient (R = 0.031) represented a small effect, while the coefficient of determination ($R^2 = 0.001$) demonstrated that PEOU only accounts for 0.1% of the variance. Furthermore, analysis of variance with ANOVA (f (.044) =0.117, p = ns) indicated that the model was a not good fit ($f< 1$), so the test was insignificant. Thus proving the null (H_0) hypothesis that PU does not have an effect on the potential adoption of online biometrics and as a result rejecting the alternate hypothesis which suggests that it does.

4.3.5 Hypothesis 4: Perceived Privacy Concern has an Impact on Potential Adoption and Use of Online Biometrics

Many users have privacy concerns when they browse/purchase on line. Many websites are implementing privacy policies and getting privacy certified by privacy-trust organisations to instil consumer confidence. To get an overall view on internet privacy, the respondents were asked the following questions in relation to online biometrics (Table 4.10).

TABLE 4.10. Privacy Concern Statement with Respect to Biometrics

Q	Storage of digitalised biometric data…?	
	S1	Is an invasion of an individual’s privacy
	S2	Could be used for other unintended purposes without my consent

Likert type responses in the Table 4.11 were combined to create a likert scale for further analysis. The overall grand mean (2.312) of the scale was used to determine the central tendency suggesting that 50% of the respondents did have the privacy concerns. With an SD of 0.77943 demonstrating that 68% of the responses are close to the mean due to a relatively narrow distribution.

Table 4.11 Privacy Concern Statement with Responses

Statements	Strongly Agree (1)	Agree(2)	Neutral(3)	Disagree(4)	Strongly Disagree(5)
S1, n=124	15	41	36	31	1
S2, n=125	34	70	15	6	0

Cronbach's alpha $(\alpha = 0.668)$ showed that the internal consistency and reliability of scale was questionable $(\alpha < 0.70)$. There were no other likert types in the survey that could be added to improve the reliability of this scale.

As with the other constructs, a simple liner regression test was performed to predict the effect that perceived privacy concern have on the potential adoption of online biometrics. In analysing the fit of the model, the correlation coefficient (R = 0.235) represented a variance effect with perceived privacy concerns accounting for 5.5% of the total variance as demonstrated by the coefficient of determination (R^2 = 0.055).

Furthermore, analysis of variance with ANOVA (f (2.555) = 7.221, p = 0.008) indicated that the model was a good fit (f ≥ 1) and the chances of getting the same result without the perceived privacy concern effect was statistically low (p < 0.5). Also, the standardised coefficient (β_1=0.235) which predicts the influencing power, indicated that for every one standard deviation change in the security concern predictor, there will be a slight increase in the adoption of biometrics by 0.235 of its standard deviation (SD = 0.60959). Given that P=0.008, this result was significant statistically thus disproving the null (H_0) hypothesis that perceived privacy concern does not have an impact on potential adoption of online biometrics and thus supporting the alternate hypothesis which suggests that it perceived privacy does indeed have an impact on potential adoption of online biometric technology.

4.3.6 Hypothesis 5: Social Influence has an Impact on Potential Adoption and Use of Online Biometrics

From the literature, the influence of others also plays a part in the adoption and use of newer technologies. This was also included in the conceptual model in this study to see if it played a role. A single item statement, as shown below, fulfilled requirements to measure this construct.

S1. I will only use biometric technology if I get positive feedback from family and friends

The responses were recoded to allow for analysis in SPSS, the same recoding as completed for testing the other constructs:-, PEOU, PU, perceived security concern, perceived privacy concern and adoption of online biometrics. However, as there is only one likert item, it was converted into ordinal data; the median was used to calculate the central tendency. Using SPSS, the median was calculated to be 3.00 (Neutral), the first quartile (Agree) and third quartile (Disagree) were calculated to get the interquartile range while demonstrates that there is wide distribution of the responses between agree and disagree. Based on this finding, the respondents on average neither agree nor disagree with the statement and this suggests that social influence might not play a major role in the adoption and use of online biometrics. However, from reviewing the frequency distribution (Figure 4.7), it is clear that 42.8% (Sum of agree and strongly agree responses) would base their adoption of online biometrics on recommendations from friends/ families.

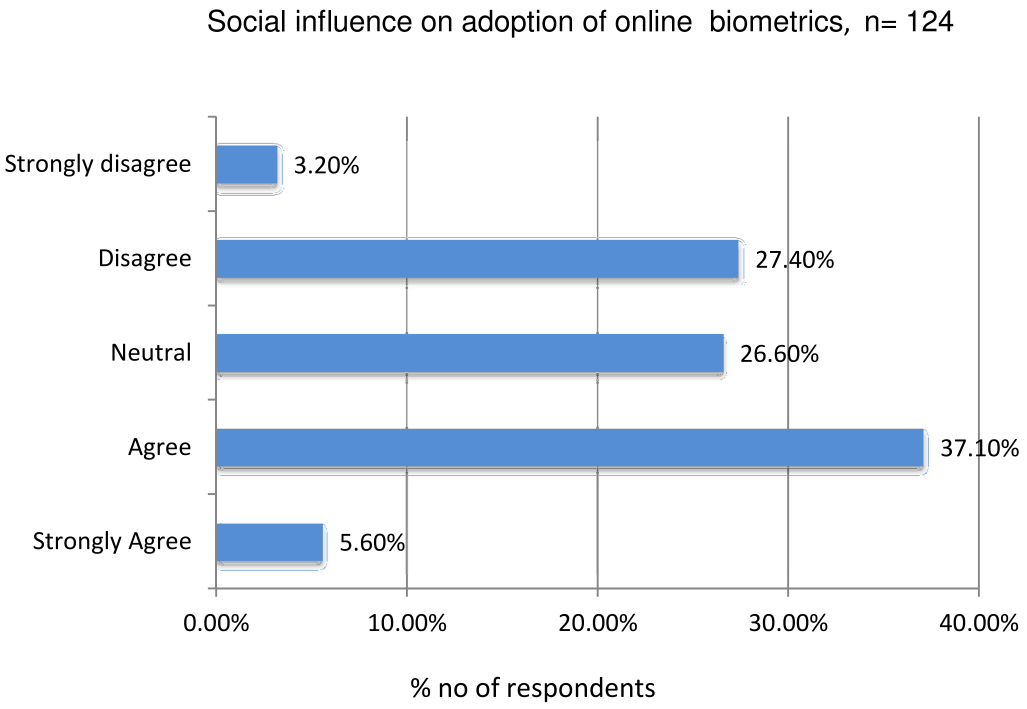


FIGURE 4.7 Social Influence on Adoption of Biometrics

To investigate further, the 5 point scales were converted into a three point scale and the resulting three groups were checked against the potential adoption construct to get the corresponding potential adoption of biometric mean (Table 4.11).

TABLE 4.12 Social influence Group Potential Adoption of Biometrics Mean

BIOMETRIC_MEAN_3

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
2.00	53	1.6101	.59101	.08118	1.4472	1.7730	1.00	3.00
3.00	33	1.9596	.61100	.10636	1.7429	2.1762	1.00	3.33
4.00	38	1.9868	.56736	.09204	1.8004	2.1733	1.00	3.33
Total	124	1.8185	.61192	.05495	1.7098	1.9273	1.00	3.33

On reviewing the mean for each category group there was a slight variation (Table 4.11), with the overall mean (1.8185) used to determine the central tendency, suggesting that

50% would be swayed by social influence. The SD (.47728) statistic showing that 68% of responses are close to this mean value. Levene's test (F(2,121) = .270, .764) indicated that there is homogeneity of variance. Further testing using Anova (f (1.082) = 5.812, p = 0.004) supports the hypothesis that social influence does have an impact on adoption of online biometrics. Using a scatterplot graph, it was found that higher social influence had a positive impact on the potential adoption and use of online biometrics.

Further analysis examined if age had an impact on the social influence construct. To determine if age has a relationship with this construct, Cross-tabulation (Table 4.12) and further testing with Chi-square (X^2 (4)=.315,0.989) analysis was performed. Even with dividing the two sided P value to get one side, the resulting value (P=0.495) was greater than 0.05 so value is not significant and relationship is not supported.

Table 4.12 Social Influence and Age Category Cross-tabulation

Count

		Age category			Total
		21-29	30-39	40-49	
Social influence	Agree	13	31	9	53
	Neutral	7	20	6	33
	Disagree	10	21	7	38
Total		30	72	22	124

4.3.7 Hypothesis 6: PEOU influence on PU

To investigate if PEOU can predict the outcome of PU, a simple liner regression was performed to predict the effect and prove the alternate hypothesis (H_6) with PU as the dependent variable. In analysing the fit of the model, the correlation coefficient (R = 0.213) represented a small effect, while the coefficient of determination (R^2 = 0.045) demonstrates that PEOU accounts for 4.5% of the variance. Furthermore, analysis of variance with ANOVA (f (2.144) =5.852, p = 0.017) indicated that the model is a good fit (f> 1), and the test was significant. In addition, the standardised coefficient (β_1=0.213) indicating that for every one standard deviation change in the PEOU predictor, there will be a slight increase in PU by 0.213 of its standard deviation (SD = 0.6107) which is not significant. As the model is a good fit and p=0.017, the result was statistically significant thus disproving the null (H_0) hypothesis the PEOU does not have an impact on PU and in doing so supporting the alternate hypothesis that it does have an influence.

4.3.8 Hypothesis 7: Perceived Privacy Concern Influence on Perceived Security Concern

Another hypothesis, as proposed by the model used in this study to be examined, is the relationship between perceived privacy concern and perceived security concern. A simple liner regression was performed to predict the effect and prove the alternate hypothesis (H_7) with perceived security as the dependent variable. In analysing the fit of the model, the correlation coefficient (R = 0.540) represented a medium effect, while the coefficient of determination (R^2 = 0.292) demonstrates that perceived privacy concern accounts for 29.2% of the variance. Further testing of the variance with ANOVA (f (18.499) =50.648, p = 0.000) indicated that the model is a strong fit (f> 1), and the test was significant.

Moreover, when testing the predictive influence of perceived privacy concern on perceived security concerns. In addition, the standardised coefficient (β_1=0.540) indicating that for every one standard deviation change in the perceived privacy concern predictor, there will increase in perceived security concern by 0.540 of its standard deviation (SD = 0.71519) which is significant. As the model is a good fit and p=0.000, the result was statistically significant thus disproving the null (H_0) hypothesis that the perceived privacy concern does not have an impact on perceived security control and in doing so supporting the alternate hypothesis that it does have an influence.

4.4 Current Online Behaviours Concerning Security, Privacy and Identify Theft

This section of the analysis identifies if those surveyed have been impacted by identity theft and what security and privacy issues they exhibit when they are online. 80.8% of the respondents have been targeted by cybercriminals using phishing emails, moreover 10% have already been victimised online (Figure 4.8). In addition, only 36.8% of respondents remove cookies after browsing, the other 63.2% being more susceptible to online theft due to malicious Trojan viruses like Zeus malware which can be used to create a third party cookie which can steal login details and personal information.

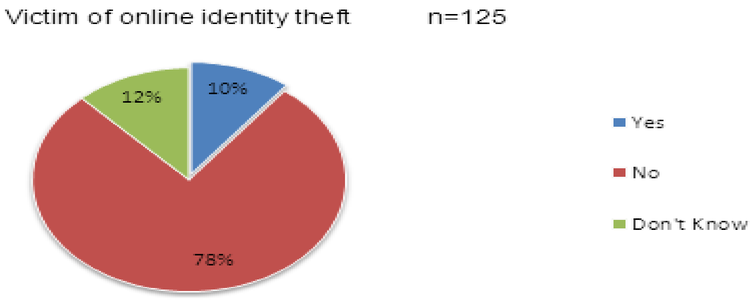


FIGURE 4.8– Online Identify Theft Victim

From the qualitative data, those that were victims suffered from financial identity theft in the form of credit card fraud, details stolen and items bought with credit card details but no goods received. In general, respondents were concerned about credit card fraud. Based on the quantitative data, 67.2% were concerned about credit card fraud (Figure 4.9)

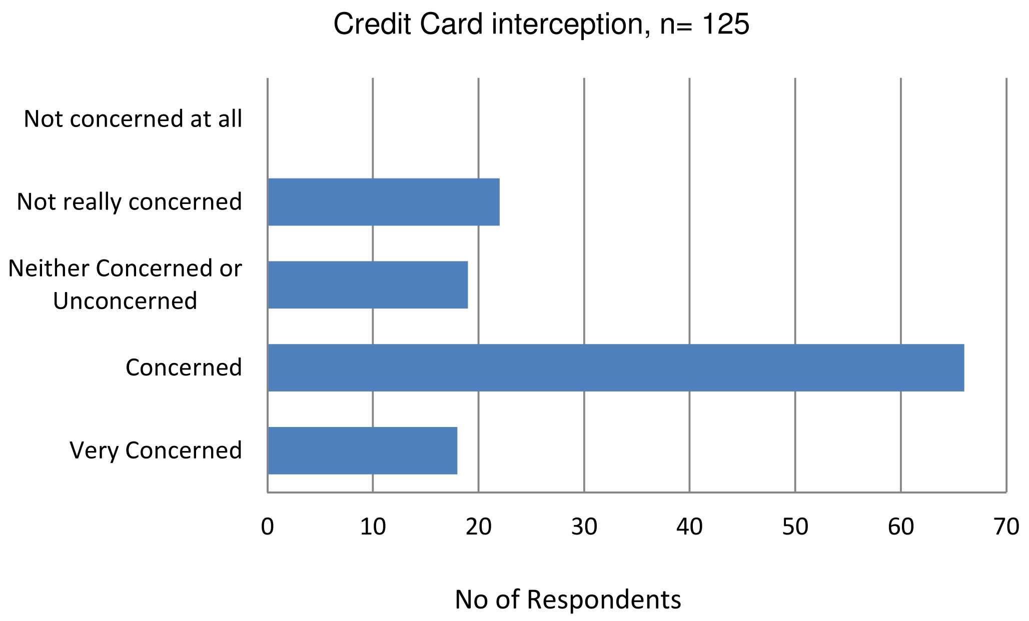


FIGURE 4.9 – Credit Card Fraud Concern

The mode of the data suggesting that the central tendency is that on average a person will be concerned about identity theft. Of those that were surveyed, the majority would use a trusted third party tool such as PayPal if it is available which offers increased security and additional protection if fraud was to occur, 47.7% would use it most of the time. When queried on the most favoured form of security protection the participants were given a number of options to choose which they ranked 1-5, where 1 was most favoured and 5 least favoured (Figure 4.12). The most favoured method of online protection was not biometric encryption which would not require your digitalised data to be stored in a location or on a cloud service, this was the second favourite; the preferred method was the combination of a biometric trait and a password.

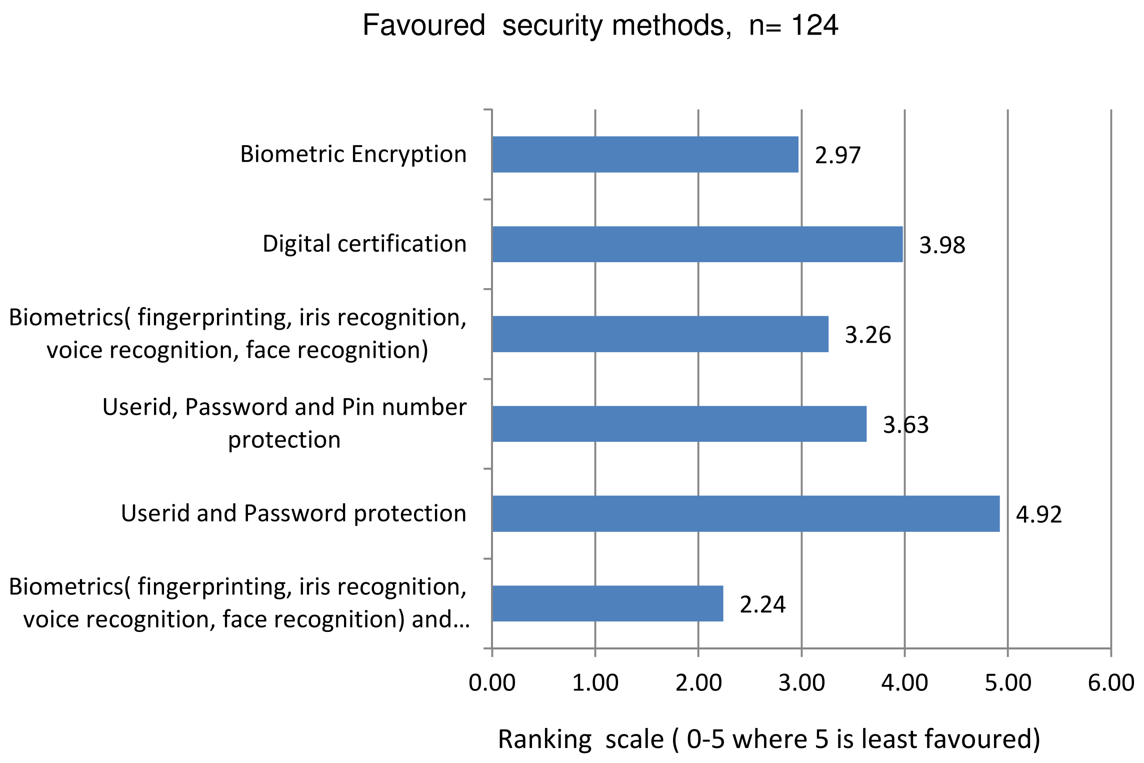


FIGURE 4.12 – Favoured Online Security Method

This is support by data gathered from the qualitative responses; a major concern was what would what would happen if an individual's biometric data was stolen and re-used.

Respondent 1:

" I would prefer the system that will minimise the number of codes and passwords I have to remember and at the same time will be a combination of the use of one or several biometrics + one key word /pin"

Respondent 2:

"Since biometric data is static once intercepted it can be used to impersonate user for life"

Concerning privacy, 64.5% are concerned that they are asked for too much information when they register online, yet it is rarely a deterrent in preventing online registration as 49.6% of respondents would still register while 32% don't know. This would need to be explored further in future research to determine why so.

5. Conclusions and Future work

5.1 Introduction

As far back as 2007, online identity theft was considered by some to be the crime of the information age (Schneier, 2007); six years on and this hasn't changed. Online biometrics has been heralded as the technology that will prevent it from occurring in the future (Kleist, 2007) yet the findings of this study suggest that when if respondents were asked if they would avoid a website that had online biometrics verification checks, 8.8% agreed while 30.4% of the respondents were undecided with the remainder disagreeing. The relatively high percentage of the neutral and agree groups combined suggesting that there are other factors at play in the decision to potentially adopt online biometrics. In the next section this will be discussed.

5.2 Discussion of Results and New Findings

After completing the literature review, a model was proposed to examine the research questions posed by this research (see, section 1.4) in particular to examine the factors that were identified as having an influence on the potential adoption of online biometrics. These five external factors being: - security concerns, privacy concern, PEOU, PU and social influence. Each hypothesis proposed by the model was tested (Figure 2.5); however, not all were proven. This analysis suggests the following refined model (Figure 5.1).

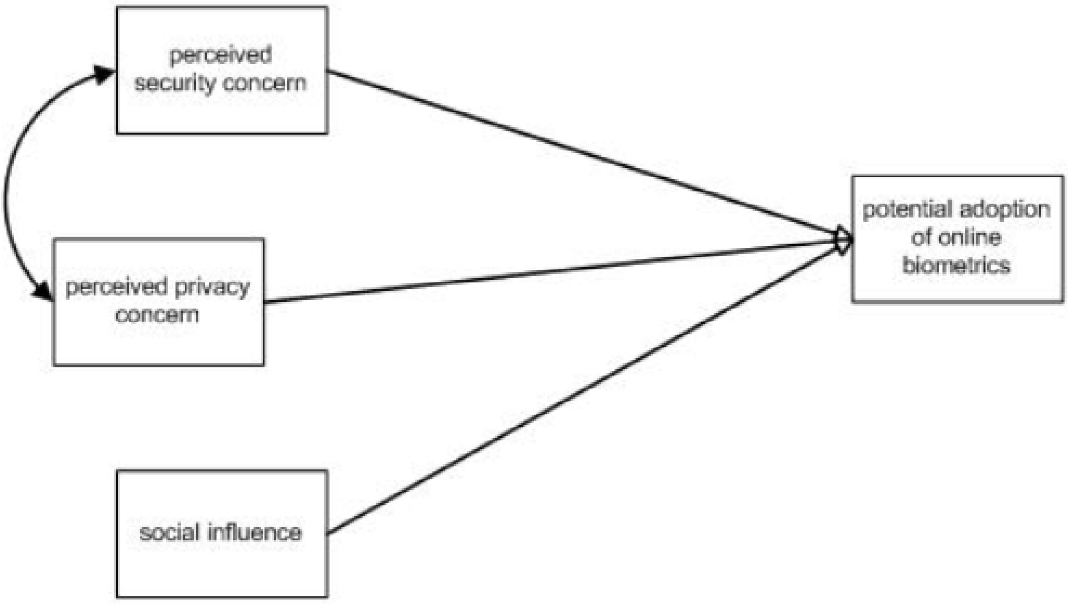

perceived security concern
perceived privacy concern
social influence
potential adoption of online biometrics

FIGURE 5.1 Revised Proposed Model to Measure Potential Adoption

Data collected from the online questionnaire was grouped according to each of the five constructs as per the original proposed model. Each constructs relationship with the adoption of biometrics was then statistically analysed using either ANOVA or linear regression. The study found that three of the independents factors do have a statistically significant impact on the potential to adopt online biometric technologies; these were perceived security concerns, perceived privacy concerns and social influence. Using ANOVA analysis, of the three, the strongest effect was social influence (p=0.004). The relationship demonstrated that respondents that will potentially adopt online biometrics are influenced by social influence of their peers and colleagues. This is a finding that was not found when reviewing literature with respect to adoption of biometrics so could be considered a new finding. Where it is has been used with respect to other technologies it was found to have an impact (Venkatesh *et al,* 2012).

Perceived privacy concern (p=0.008) has a stronger effect that perceived security concern (p=0.012). After, using a scatterplot graph, it was found that those that had the highest privacy concerns about online biometrics were actually more likely to potentially adopt this technology than those who were not as concerned. A similar result was also found for the impact of perceived security concerns on potential to adopt online biometrics, where those with the highest security concern were more likely to adopt this technology. Neither of these results were expected; while research in this field of online biometrics is limited, a previous study completed using the construct perceived risk (Keng Lin *et al,* 2010) found that an increase in perceived risk negatively affected the intention to use online biometric. Lu *et al* (2005) also found that perceived risk associated with technologies did negatively impact intentions to use it. So the two results found in this study will have to be explored further in future research to examine why this is so. One possible explanation is that the respondent's with the highest level of privacy and security concerns are generally more aware of the hidden dangers of the internet and this alone is why they would want to adopt and use online biometrics solution as a verification system when they are purchasing online; for those individuals, the benefits exceed the risk.

A linear regression was used to further examine the relationships that perceived security concerns and perceived privacy concerns have on the potential adoption of online biometrics. It was found that perceived privacy concern has the highest influencing power with a beta coefficient of 0.235 compared to 0.233 for perceived security concern. As none of the literature reviewed examined these two factors as separate constructs in the same study, it is not possible to compare and identify if this is the case with other studies. However, as can be seen from the beta coefficient values, the difference in influencing behaviour is small and could be consider insignificant.

Moreover, a relationship was found to exist between perceived privacy concern and perceived security concern. However, although the linear regression analysis shows there is a relationship between these constructs, it is not possible to determine the cause or direction of the relationship. This would need to be explored further using a longitudinal study. Qualitative data collected also supports this relationship that in a lot of cases, respondents mentioned security and privacy concerns in tandem in relation to purchasing online and adoption of biometrics

An interesting new finding which was not evident from the literature reviewed is the impact of internet performance on security behaviour; it was found that 25% of those surveyed do in fact switch off their security settings to improve overall performance. Delving deeper into the data, of those who do disable security settings, 80% were those who allowed for automatic security updates suggesting that performance is certainly a factor in online behaviour with those switching off security features in reality not being very security conscious.This raises a concern around security in general, while people do have concerns about fraud, they do take unnecessary risks to get the item they so desire regardless of consequence; this may be due to the fact that they are under the impression that financial institutions will repay their losses if fraudulent activity is found on their card regardless of the activity.

Both the PEOU (p=0.134) and PU (f=0.177) constructs were found to have insignificant impact on the potential adoption of online biometrics. The PU model relationship with potential to adopt online biometrics was not deemed a model fit for analysis while PEOU was but no significant relationship was found. Both of these constructs had good scale reliability; based on previous studies using TAM (Lee *et al*, 2003) and a study previously mentioned concerning the adoption of biometrics (Keng Lin *et al,* 2010). It was expected that they both would have an impact on the potential to adopt online biometric technology. This finding would need to be explored further to determine as the Author of this dissertation expects, that concern of identity theft negates the impact of perceived usefulness and perceived ease of use of online biometric technology. This is supported by qualitative findings from this dissertation where less than 6% responded that ease of use and perceived usefulness were factors in the adoption of biometrics.

Other new findings that were not evident in the literature review were that the majority of the respondents were concerned about online identity theft (90.4% of respondents) and of the different mechanisms reviewed; a biometric only system of verification was not preferred. Respondents are still in favour of two-factor authentication but with biometrics as an integral part of this. The favoured biometric trait being fingerprint verification systems. Of interest is that biometric encryption was expected to be best solution, as it would not require digitalised data to be stored online, however as noted in the qualitative data, there were many concerns raised about the aftermath of stolen biometric data, so it is possible the respondents feel more secure that a pin number would also be required for additional security in case biometric data was stolen.

5.3 Benefit of Research

The new findings already discussed will add to the existing body of knowledge with respect to the adoption of online biometric technology. Moreover, the proposed model is another model that can be used in its current form or enhanced to identify if people from other demographics would potentially adopt online biometric technology.

5.4 Generalisability of Findings

While this study is of interest to the public and to companies involved in the online biometric industry, it is not possible to generalise the findings for the following reasons: -

- The over 40 category group had less than the recommended thirty responses for generalisation (Stutely, 2003).
- The sample size was small and convenience sampling was used

Taking Stutely's recommendation into account, the over 40 category would have to be excluded if the study was to be generalised. To do so, would have an impact on the overall findings of this study as this category was sizeable, accounting for 17.6% of the respondents from the internet community. Moreover, as a targeted convenience sampling was used to get responses from the sample frame, it cannot be considered as being representative of the Irish internet population. To be considered, sampling would have to be randomised and sample size would have to increase in order to lower the probability of error when generalising to the population (Saunders *et al*, 2009).

5.5 Limitations of Research

While the findings of this study have identified security and privacy concerns as well as social influence as being key factors which impact the adoption of online biometrics, there are some limitations with the study. The PEOU construct used in the study had poor scale reliability. It was found to have a cronbach's alpha value ($\alpha<0.5$) less than what is recommended for use in studies. In addition, the potential adoption of biometrics construct had questionable scale reliability.

Poor scale reliability can impact the result outcome and as noted in the results discussion, the result outcome from examining the relationship between PEOU and adoption of biometrics could be flawed as a result of the poor scale reliability. Due to time limitations it was not possible to redesign the constructs to improve the scale reliability and in doing so increase the accuracy of the results, nor was it possible to do a longitudinal study to determine the extent of the relationships between the five constructs and adoption of biometrics and themselves over time which may lead to differing but more meaningful results.

Moreover, another limitation is that online biometrics is still an emerging technology; a finding of this dissertation was that 38.7% of those surveyed did not have any prior knowledge of online biometrics systems. If all respondents had some level of knowledge and experience with this technology there could be a different result outcome. Finally also, due to time constraints, interviews and group studies were not deployed. On comparing the qualitative and quantitative data, it was found that while respondents are generally concerned about security and privacy, they act very differently when on the Internet; with 25% switching off their security settings to improve performance.

5.6 Future Research Opportunities

As online biometrics is an emerging field there is ample opportunity for further research: based on the both the quantitative and qualitative findings of this study, the following areas of interest could be investigated further:

5.6.1 Security and Privacy relationship

While the finding of this study suggests that privacy and security concern have an impact on the potential to adopt online biometrics. This study also highlighted the fact that the respondent's current online behaviour did not always reflect this concern. Though 90.4% of those surveyed were concerned about identity theft, 25% switched off security settings to improve performance and 46.6% would register their details regardless of any privacy concerns to purchase the item they require.

So with respect to security and privacy concerns, exploring this relationship further would be of interest not only to companies that are launching online biometric solutions but also the online security research field. Points of interest being, firstly, what level of privacy are the general public willing to trade for increased security online and secondly, what level of control would they need over their digitalised data before they agree to enrol it with an online verification system. Neither of which were explored in this study.

One individual suggested that before they would use online biometrics he/she would require 'Confirmation that my biometrics data is my property and I have the right to request it to be deleted from the vendor service when required''.

5.6.2 Impact of Credibility and Performance

Another area of interest is to explore the impact perceived accuracy and perceived performance may have on the credibility and adoption of an online biometric verification system. As mentioned in the literature review, with biometric verification systems a threshold must be achieved before a person is verified to be whom they say they are. There are two types of errors mainly associated with this:-

1) False rejection rates

2) False acceptance rates.

Both of these errors have an impact on the system accuracy (Wayman and Mansfield, 2002). Given that these errors could exist with a biometrics solution and that there is an inverse relationship between the two (Ngugi *et al*, 2011) i.e. a decrease in a false acceptance error would result in an increase in a false rejection rate and vice versa. It would be interesting to examine which error type would more negatively impact the adoption of the online biometrics by the general public and what level accuracy would be tolerated. Ngugi et al have already attempted to measure the influence of these two error types with their Intention to use biometric systems model (Ngugi *et al,* 2011). As a follow on from this research, the proposed model in this study could be enhanced with a false rejection rate and a false acceptance rate construct and their influence on the potential to adopt online biometrics.

Another construct to add to this proposed model is performance. To have a system with low false acceptance errors would require a complicated algorithm which would impact performance (Wayman and Mansfield, 2002). As 25% of those surveyed in this study have switched off security settings to improve performance online, it would be interesting to see how influential poor performance would be on the adoption of online biometrics. Would individuals avoid purchasing from websites that had a biometric system with increased accuracy but with poor performance; - this would also be of interest to online retailers thinking of using biometric verification as a means of identification.

5.6.3 Longitudinal Research to Measure Adoption of Online Biometrics

To further research completed in this study, it would be interesting to repeat the study a number of times to get a diary perspective on the relationship rather than a snapshot as was done in this study using an enhanced version of the revised mode which would include the performance and perceived credibility constructs mentioned in section 5.6.2.

As mentioned in the literature review, fingerprint biometrics is currently identified as being the best fit for online biometrics and this was supported by findings in this study; however until people actually use the systems it is impossible to say without any degree of uncertainty which one is fit for purpose. The purpose of this longitudinal research would be to examine changes in behaviour over a period of time as respondents are exposed to different online biometric technologies – sessions would be held to allow them to use the available solutions and gain practical experience with the aim to identify the biometric system which in the eyes of the public is the best fit and in doing so identify the key factors that may have a long lasting impact on the adoption of this technology.

5.6.4 Selection of Biometric Method

From this study, without having hands on experience of online biometrics and 37.8% of respondents having no knowledge of biometric systems, the security method of choice was chosen to be biometrics and pin which was seen as the most secure. This would need to be explored further especially given the concern raised about the storage of data and the fact that biometric encryption solutions would also be available. The findings from this research would be of interest to the companies involved in the online biometric industry as it will give them an indication of the direction they should be following with their solution.

Another avenue of research would be to complete a focus group study giving them unbiased end user perceptions of the advantages and disadvantages of each solution to identify whether or not biometric encryption solutions (where your biometric data is used to unlock a security key) are viable options to the storage of biometric data online. They could also be asked to fill out a quantitative questionnaire based on the revision of proposed model used in this research to measure the potential adoption of each solution. . The influence of age should also be examined to see if it has impact on the solution adopted or is it age independent given the most people in 20-60 age group are familiar with the internet and how it operates in terms of purchasing.

5.7 Summary

In summary, the questions posed by this dissertation were answered;- factors influencing adoption of biometrics were identified, fingerprint technology was seen as the best fit for online verification and it was also determined that biometrics alone would not be the preferable choice to prevent identity theft. It has been a very interesting and rewarding study not only for the author but also for those that participated with a number of respondents rethinking their online behaviour after completing the online survey for this dissertation. Finally, based on results obtained in this study, the majority of respondents are willing to adopt online biometric technology to prevent identity theft.

6. Bibliography

Agarwal, R, & Karahanna, E 2000, 'TIME FLIES WHEN YOU'RE HAVING FUN: COGNITIVE ABSORPTION AND BELIEFS ABOUT INFORMATION TECHNOLOGY USAGE', *MIS Quarterly*, 24, 4, pp. 665-694, Business Source Complete, EBSCO*host*, viewed 01 June 2013.

Ahmed, F. and Siyal M.Y (2005)- A novel approach for regenerating a private key using password, fingerprint and smart card. *Information Management & Computer Security*

AJZEN, I. AND M. FISHBEIN (1980), *Understanding Attitudes and Predicting Social Behaviour.* Prentice-Hall, Englewood Cliffs, NJ.

Ajzen, I., (1985), "From Intention to Actions: A Theory of Planned Behavior," in Kuhl, J and Bechmann, J (Eds.), *Springer Series in Social Psychology*, Berlin, Springer.

Ajzen, I, & Fishbein, M 1972, 'Attitudes and normative beliefs as factors influencing behavioral intentions', *Journal Of Personality And Social Psychology*, 21, 1, pp. 1-9, PsycINFO, EBSCO*host*, viewed 05 June 2013.

Ajzen, I. (1991) The theory of planned behavior, "Organizational Behavior and Human Decision Processes", Vol. 50, pp 179-211.

Ajzen, I 2001, 'Nature and operation of attitudes', *Annual Review Of Psychology*, 52, pp. 27-58, PsycINFO, EBSCO*host*, viewed 10 May 2013.

Bélanger,F; Crossler, R.E. Privacy in the digital age: A review of information privacu research in information systems MIS Quarterly, v. 35, n. 4, 2011 p. 1017-A36, Available http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=67123613&site=ehost-live (Accessed: 12 july 2013).

Bolle, R.M, Connell j.h, Pankanti, S., Ratha, N.K & Sention, A.w (2004) Guide to biometrics. New York: Soringer-verlag

Boone, D., and Boone, H. (2012) Analysising liket data.[online]
Availble at (http://www.joe.org/joe/2012april/tt2.php). [Accessed 2ND July 2013]

Bram,T., 2013. The Underground Internet Economy Of Cybercrime.[online]

Available at: <http://www.investopedia.com/financial-edge/0113/the-underground-internet-economy-of-cybercrime.aspx> [Accessed 1st June 2013].

Brooke, J. (1996). SUS: A “quick and dirty” usability scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester, & A. L. McClelland (Eds.), Usability evaluation in industry. London: Taylor and Francis. Available from http://www.usabilitynet. org/trump/documents/Suschapt.doc (Accessed 11.5.2013)

Buchanan, T, Paine, C, Joinson, A, & Reips, U 2007, 'Development of measures of online privacy concern and protection for use on the Internet', *Journal Of The American Society For Information Science & Technology*, 58, 2, pp. 157-165, Business Source Complete, EBSCO*host*, viewed 27 April 2013

Crosby,J., 2008. Challenges and opportunities in identity assurance.[online]
Available at: http://www.statewatch.org/news/2008/mar/uk-nat-identity-crosby-report.pdf.
[Accessed 1st June 2013]

Curran,J. and Blackburn, R.A. (2001) *Researching the Small Enterprise*. London: Sage.

DAVIS, F. D., "A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results," Doctoral dissertation, Sloan School of Management, Massachusetts Institute of Technology, 1986.

Davis, FD 1989, 'Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology', *MIS Quarterly*, 13, 3, pp. 319-340, Business Source Complete, EBSCO*host*, viewed 5 May 2013.

Davis, FD 1989, 'Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology', *MIS Quarterly*, 13, 3, pp. 319-340, Business Source Complete, EBSCO*host*, viewed 5 May 2013.

Davis, F, Bagozzi, R, & Warshaw, P 1989, 'USER ACCEPTANCE OF COMPUTER TECHNOLOGY: A COMPARISON OF TWO THEORETICAL MODELS', *Management Science*, 35, 8, pp. 982-1003, Business Source Complete, EBSCO*host*, viewed 1 May, 2013

Davies, S,G (1994) Touching Big brother: How biometric technology will fuse Flesh and machine. Information Technology & People 7(4):38-47

Deutskens, E., de Ruyter, K., Wetzels, M. & Oosterveld, E (2004) Response rate and response quality of internet-based surveys: an experimental study. *Marketing Letters,* 15, 1, pp. 21-36.

Dinev, T., and Hart, P. Privacy concerns and Internet use - A model of trade-off factors. In *Best Paper Proceedings of Annual Academy of Management Meeting.* Briarcliff Manor, NY: Academy of Management, 2003, pp. 131–137

Dinev, T., and Hart, P. Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behaviour and Information Technology, 23*, 6 (2004), 413–423.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for e-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.v

Doyle,C., 2012. European Cybercrime Centre to crack down on cyber threats.[online] Available at:<http://www.siliconrepublic.com/strategy/item/26584-european-cybercrime-centre>. [Accessed 5th June 2013]

Dunn,J.E., 2012a. Gang jailed for running £11 million ID theft 'fraud factory.[online]
Available at:
http://news.idg.no/cw/art.cfm?id=A1235C83-B7B3-09EC-EB1285BED9DBB09 [Accessed 28th May, 2013].

Dunn,J.E., 2012b. Attack on airport VPN bypassed multi factor authentication security firm reports.[online]
Available at: http://news.techworld.com/security/3375826/attack-on-airport-vpn-bypassed-multi-factor-authentication-security-firmreports/? [Accessed 2ND June 2013]

European Commission, 2012a. Special Eurobarometer390-Cyber Security. [online]
Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf [Accessed 7th may 2013].

European commission, 2012b. Cracking down on cybercrime, [online]
Available at: http://ec.europa.eu/news/justice/120328_en.htm [Accessed 1ST June 2013].

Evans, Joel, R. Mathur (2005), The value of online surveys. Anil Internet Research Vol. 15, No. 2, p. 195-219

Fishbein, M., and Ajzen, I., (1975), *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Addison-Wesley, Reading, MA.

Fischer,T (2007) Securing the online world with biometrics, Biometric Technology Today, Volume 15, Issue 6, June 2007, Page 7, ISSN 0969-4765, (http://www.sciencedirect.com/science/article/pii/S0969476508700377)

Fujun Lai, Dahui Li, Chang-Tseh Hsieh, Fighting identity theft: The coping perspective, Decision Support Systems, Volume 52, Issue 2, January 2012, Pages 353-363, Available at http://www.sciencedirect.com/science/article/pii/S0167923611001588 (Accessed: 10 Jun 2013)

G.R. Milne, A.J. Rohm, S. Bahl, Consumers' protection of online privacy and identity, Journal of Consumer Affairs 38 (2) (2004) 217–232.

Gokulkumari, G, & Lakshmi, A 2011, 'Study of Effects and Perceptual Analysis in Implementing Biometric Authentication', *European Journal Of Scientific Research*, 61, 2, pp. 242-254, Academic Search Complete, EBSCO*host*, viewed 29 August 2013

Ilieva, J., Baron, S. & Healey, N.M. (2002) Online surveys in marketing research: pros and cons.*International Journal of Market Research,* 44, 3, pp. 361-382

Introna, L.D., & Pouloudi, A. (1999). Privacy in the information age:
Stakeholders, interests and values. Journal of Business Ethics, 22, 27–38.

Jain, A.K (2004). *Biometric recognition: How do I know who you are. IEEE Symposia, 3-5*

Jain, A., and Ross, A.(2008). “Introduction to Biometrics,” in Handbook of Biometrics, A.Jain, P.Flynn and A.Ross,(eds), New York:Springer,pp. 1-22

James, T., Pirim, T. Bowell, K., Reithel, B, and Barkhi,R (2006). Determining the intention to use biometric devices: An application and extension of the technology acceptance model. Journal of Organisational and End user computing, 18(3):1-24

Javelinstrategy, 2013. 2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters.[online] Available at: https://www.javelinstrategy.com/brochure/276. [Accessed 28th May 2013]

Jupp, V. (2006), *The sage dictionary of social research methods / compiled and edited by Victor Jupp* SAGE Publications London ; Thousand Oaks, Calif

Keng Lin, S, WaiPeng, W, & Kok Leong, C 2010, 'Adoption of Biometric Technology in Online Applications', *International Journal Of Business & Management Science*, 3, 2, pp. 121-146, Business Source Complete, EBSCO*host*, viewed 29 August 2013.

Kleist, V 2007, 'Building Technologically Based Online Trust: Can the Biometrics Industry Deliver the Online Trust Silver Bullet?', *Information Systems Management*, 24, 4, pp. 319-329, Business Source Complete, EBSCO*host*, viewed 18 May 2013.

Lee, Y, Kozar, K, & Larsen, K 2003, 'THE TECHNOLOGY ACCEPTANCE MODEL: PAST, PRESENT, AND FUTURE', *Communications Of AIS*, 12, pp. 752-780, Business Source Complete, EBSCO*host*, viewed 5 August 2013.

Legris, P., Ingham, J., and Collerette, P., (2003), “Why do People Use Information Technology? A Critical Review of the Technology Acceptance Model,” *Information and Management*, 40, p. 191-204.
(http://www.sciencedirect.com/science/article/pii/S0378720601001434)

Lu,J., H.P.,Hsu, C.L and Hsu, H.Y (2005). An empirical study of the effect of perceived risk upon intention to use online applications. Information Management & Computer security, 13(2):106-120.

Lozar Manfreda, K., Bosnjak, M., Berzelak, J., Haas, 1. & Vehovar, V (2008) Web surveys versus other survey modes: a meta-analysis comparing response rates. *International Journal of Market Research,* 50, 1, pp. 79-104.

MacLeod, C 2005, 'Password overload syndrome?', *Back Office Focus*, 113, pp. 11-12, Business Source Complete, EBSCO*host*, viewed 07 August 2013.

Maguire, M 2009, 'The birth of biometric security', *Anthropology Today*, 25, 2, pp. 9-14, Academic Search Complete, EBSCO*host*, viewed 4 August 2013.

Malhotra, N, Sung S., K, & Agarwal, J 2004, 'Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model', *Information Systems Research*, 15, 4, pp. 336-355, Business Source Complete, EBSCO*host*, viewed 29 August 2013.

Mason, RO 1986, 'Four Ethical Issues of the Information Age', *MIS Quarterly*, 10, 1, pp. 5-12, Business Source Complete, EBSCO*host*, viewed 30 August 2013.

Matsumoto,T., et al ‘Impact of Artifical ‘Gummy’ fingers on Fingerprint Systems’ proceedings of SPIE Optical Security and Counterfit Deterrence Techniques iv, 2002

Milne, G, Rohm, A, & Bahl, S 2004, 'Consumers' Protection of Online Privacy and Identity', *Journal Of Consumer Affairs*, 38, 2, pp. 217-232, EconLit with Full Text, EBSCO*host*, viewed 29 August 2013.

Modi, Shimon K (2011) ‘Fundamentals of Technical Evaluations’, in Modi (ed), Biometrics in Identity Management: Concepts to Applications. pp 7-8.

Khalil-Hani, M., Marsono,M., Bakhteri,R.,(2013) Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm, Future Generation Computer Systems, Volume 29, Issue 3, March 2013, Pages 800-810, ISSN 0167-739X, (http://www.sciencedirect.com/science/article/pii/S0167739X12000350)

Nanavanti, S., Thieme, M.,& Navavati, R (2002) . Biometrics: Identity verification in a networked world New York: John Wiley & Sons, Inc.

Ngugi, B, Kamis, A, & Tremaine, M 2011, 'Intention to Use Biometric Systems', *E-Service Journal*, 7, 3, pp. 20-46, Business Source Complete, EBSCO*host*, viewed 29 August 2013.

O’Neil, D. (2001) Analysis of Internet users’ level of online privacy concerns. *Social Science Computer Review, 19*, 1 , 17–31.

Obaidat,M. & Boudriga,N. eds, 2007 – Biometric-based system in Security of e-systems and computer networks, Cambridge University Press, New York,NY,USA

Organisations for Economic Co-operation and Development (2008), Scoping paper on online identity theft .Available at, http://www.oecd.org/dataoecd/35/24/40644196.pdf.

(last accessed 12th Jun, 2013)

Paul, I., 2013. Online security: your two-factor authorization checklist.[online]
Available at: <http://www.pcworld.com/article/2036298/online-security-your-two-factor-authorization-checklist.html> [Accessed 8th July,2013]

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

(Spring 2003), 101–134.

Pavlou, PA 2011, 'STATE OF THE INFORMATION PRIVACY LITERATURE: WHERE ARE WE NOW AND WHERE SHOULD WE GO?', *MIS Quarterly*, 35, 4, pp. 977-988, Business Source Complete, EBSCO*host*, viewed 01 May 2013.

Ramaswamy, VM 2006, 'Identity-Theft Toolkit', *CPA Journal*, 76, 10, pp. 66-70, Business Source Complete, EBSCO*host*, viewed 23 July 2013.

Rashid, F., 2013. Zeus Trojan Makes a Comeback After Months of Silence.[online]
Available at:http://securitywatch.pcmag.com/malware/311889-zeus-trojan-makes-a-comeback-after-months-of-silence.[Accessed 10th June 2013]

Reid, Paul, (2003) – Biomertics for Network Security, Prentice Hall PTR.Upper Saddle River, NJ,USA.

Roztocki, N. (2001) Using the integrated activity-based costing and economic value added information system for project management. *AMCIS 2001 Proceedings.* Paper 282.

Saunders, M., Thornhill, A., Lewis,P.,(2009) eds. Research Methods for Business Students, 5th ed., Harlow. Pearson Education

Saunders, K, & Zucker, B 1999, 'Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act', *International Review Of Law, Computers & Technology*, 13, 2, pp. 183-192, Business Source Complete, EBSCO*host*, viewed 23 July 2013.

Schneier, B.(2007) Solving Identity Theft [online]
Available at:
:http://www.forbes.com/2007/01/19/identitiy-theft-security-cz_bz_0122identity.html
[Accessed 21th Aug 2013]

Sheppard, B, Hartwick, J, & Warshaw, P 1988, 'The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research', *Journal Of Consumer Research*, 15, 3, pp. 325-343, Business Source Complete, EBSCO*host*, viewed 5 August 2013.

Smith, J.H., Milberg, S.J., & Burke, S.J. (1996). Information privacy:Measuring individuals concerns about organizational practices. MIS Quarterly, 20, 167–196.

Smith, Russell G. (2010) ‘Identity theft and fraud’, in Jewkes,Y and Yar, M (ed), Handbook of Internet Crime, Willan Publishing, pp. 274

Smith, H. J. Dinev, T., and Xu, H. 2011. “Information Privacy Research: An Interdisciplinary Review,” *MIS Quarterly* (35:4), pp. 989-1015.

Stewart, K, & Segars, A 2002, 'An Empirical Examination of the Concern for Information Privacy Instrument', *Information Systems Research*, 13, 1, pp. 36-49, Business Source Complete, EBSCO*host*, viewed 29 August 2013.

Stutely,M.(2003) Numbers Guide:The Essentials of Business Numeracy.London: Bloomberg Press.

Suddaby, R(2006) ‘From the editors: what grounded theory is not’, Academy of Management journal, Vol.49, No.4 pp 633-42

Taylor, S, & Todd, P 1995, 'Understanding Information Technology Usage: A Test of Competing Models', *Information Systems Research*, 6, 2, pp. 144-176, Business Source Complete, EBSCO*host*, viewed 29 August 2013.

Tashakkori, A. and Teddlie, C.(eds) (2003) Handbook of Mixed Methods in Social and Behavioural Research.Thousand Oaks,CA. Sage.

Tassabehji,R., Kamala,M.(2012), Evaluating biometrics for online banking: The case for usability, International Journal of Information Management, Volume 32, Issue 5, October 2012, Pages 489-494, ISSN 0268-4012, http://dx.doi.org/10.1016/j.ijinfomgt.2012.07.001.
(http://www.sciencedirect.com/science/article/pii/S0268401212000898)

Thalheim,L.,J.Krissler, and P.M.Ziegler, Body Check: Biometric Access Protection Devices and Their Programs Put to the Test , 2002)

Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. J. 2006. “Concern for Information Privacy, Risk Perception and Online Consumer Purchasing,” *Journal of the Association for Information Systems* (7:6), pp. 415-444.

Venkatesh, V 2000, 'Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model', *Information Systems Research*, 11, 4, p. 342, Business Source Complete, EBSCO*host*, viewed 29 August 2013.

Venkatesh, V, & Davis, F 2000, 'A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies', *Management Science*, 46, 2, p. 186, Business Source Complete, EBSCO*host*, viewed 29 August 2013

Venkatesh, V, Morris, M, Davis, G, & Davis, F 2003, 'USER ACCEPTANCE OF INFORMATION TECHNOLOGY: TOWARD A UNIFIED VIEW', *MIS Quarterly*, 27, 3, pp. 425-478, Business Source Complete, EBSCO*host*, viewed 29 August 2013.

Venkatesh, V, & Bala, H 2008, 'Technology Acceptance Model 3 and a Research Agenda on Interventions', *Decision Sciences*, 39, 2, pp. 273-315, Business Source Complete, EBSCO*host*, viewed 29 August 2013

Warren, S., & Brandeis, L.D. (1890). The right to privacy. Harvard Law Review, 4, 193–220.

Wayman,J. Fundamentals of biometric authentication technologies. Int.J. Imaging and Graphics, 1(1)2001

Wayman, J.L, Technical testing and evaluation of biometric identification devices, in A.Jain, et al (eds) Biometrics: Personal Identification in Networked Society. Kluwer Academic Press, 1999.

Wayman, J.L, and T.J. Mansfield, (2002). Best Practices in Testing and Reporting Performance of Biometric Devices, Middlesex, U.K.: National Physical Laboratory

Wolff,I., 2007. Identity Theft.[online]
Available at: <http://www.sans.org/reading-room/whitepapers/awareness/identity-theft-1806> [Accessed 13th June 2013]

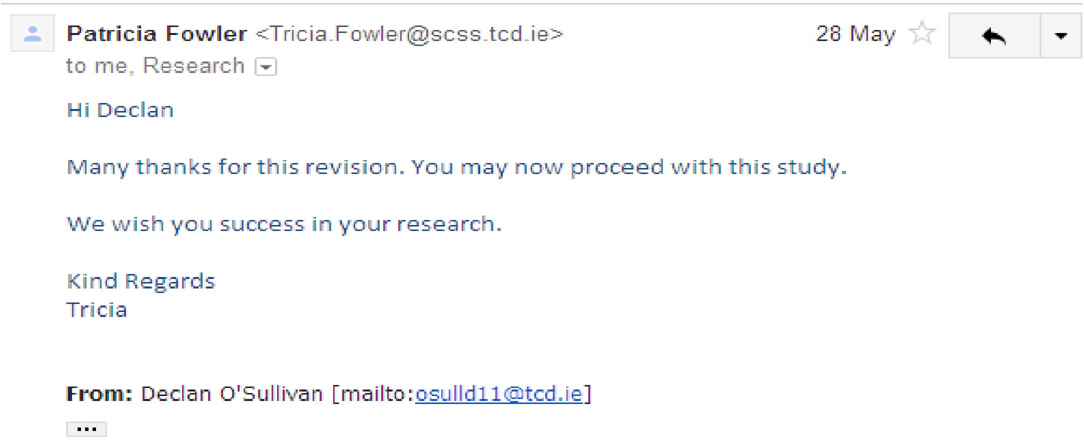
Appendices:

Appendix A

Ethical requirement was further fulfilled by having a declaration page at the start of the survey; respondents were informed and asked for their consent of the following:-

- that the participant understood there was complete anonymity and no personal details would be shared
- that the participant understood that each question with the exception of agreeing to the declaration was optional
- that the participant understood third parties could not be reference and if they were, would be anonymised
- that the participant understood Illicit activities would be reported to appropriate authorities
- that the participant understood they were 18 years or older and competent to provide consent
- that the participant understood their data would be used for scientific purposes and their data could be published which would not identify them
- that the participant understood they could refuse to answer any question and withdraw from the survey at any time
- that if the participant or a member of their family suffer from a history of epilepsy, they are proceeding at their own risk
- that the participant freely and voluntarily agrees to be part of this research study, though without prejudice to his/her legal and ethical rights.
- that the participant has read and understood the declaration and has had the opportunities to ask questions which were answered to their satisfaction

Ethics Approval received on the 28th May



Patricia Fowler <Tricia.Fowler@scss.tcd.ie> 28 May
to me, Research

Hi Declan

Many thanks for this revision. You may now proceed with this study.

We wish you success in your research.

Kind Regards
Tricia

From: Declan O'Sullivan [mailto:osulld11@tcd.ie]

...

TRINITY COLLEGE DUBLIN

EMAIL FOR SURVEY PARTICIPANTS

Hi,

My name is Declan O'Sullivan and I am a student in the School of Computer Science and Statistics, at Trinity College Dublin. I am researching the factors affecting the adoption of online biometric verification system that would offer increased security when procuring goods and services and I am inviting participants to complete an online survey, to garner opinions on this new technology. The survey forms part of my final year research project for my masters in the Management of Information Systems.

The survey is online and takes no longer than 15 minutes to complete. I hope that you will find this an interesting exercise and it will help me in completing my research which will contribute to our understanding of consumer's intention to use emerging technologies, such as online biometric verification. I would be very grateful if you could take the time to complete the survey.

The web link to the online survey is:

https://www.surveymonkey.com/s/HB7BVSQ

I attach an information sheet for survey participants, which explains the background to the research, the procedure, important notes and what happens to the survey findings.

Should you have any questions please do not hesitate to contact me.

Kindest Regards,

Declan O'Sullivan

TRINITY COLLEGE DUBLIN

INFORMATION SHEET FOR SURVEY PARTICIPANTS

BACKGROUND OF RESEARCH:

This research relates to the adoption of online biometric verification systems. A survey will be conducted with consumers to garner their opinion of this technology. Your participation in this research will make a contribution to our understanding of consumer's intention to use emerging technologies, such as Biometrics systems.

THE SURVEY PROCEDURE

The survey consists of two parts. Part one contains the informed consent form and you will be asked if you satisfy the terms and conditions listed. Part two contains a series of statements related to the participant's intention to use biometrics and also examines security and privacy concerns. The participant is asked to read each statement and rate their agreement/disagreement on a 5 point Likert scale, where 1 equates to "Strongly Disagree" and "5" equates to "Strongly Agree" and a simple yes/no to others, there are also questions where the user can select an answer from a defined list, as well a series of questions which have a comment box. There is also a request for demographic information. The following points should be noted about the survey:

- The participant has the right to withdraw from the survey at any time during the process without penalty;
- The participant may omit individual responses without penalty;
- Completion of the survey should take no more than 15 minutes;
- Since this research involves viewing materials via a computer monitor the participant should understand that if they or anyone in their family has a history of epilepsy then they are proceeding at their own risk.
- If the participant is a work colleague, then it is important to note that no workplace penalties will be experienced by non-participants and conversely no workplace benefits will be given to participants in the survey.

THE RESULTS

Once the survey has been completed, the answers will be analysed and interpreted. All information and results will be used anonymously in this analysis, as well as in the publication and presentation of data and findings. If you wish, you may receive an electronic copy of the research dissertation by contacting me at osulld11@tcd.ie , after 1st September 2013.

OTHER INFORMATION:

- This information is being gathered for the completion of a dissertation as part of the M.Sc. in Management of Information Systems.
- I have no conflict of interest with regard to the research topic or with any of the participants.
- I am required by TCD to inform you that, if in the course of the survey, you inadvertently reveal illicit activities; I must report them to the appropriate authorities.

TRINITY COLLEGE DUBLIN

EMAIL FOR HR MANAGER

Dear Eoin

I am working on a final year research project for my masters in the Management of Information Systems at Trinity College Dublin. I am researching the factors impacting the adoption of online biometric security. I would like to request permission to distribute the survey to my work colleagues at Kerry group in Northwood. The survey is online and takes no longer than 10 minutes to complete.

I have attached the following documents:

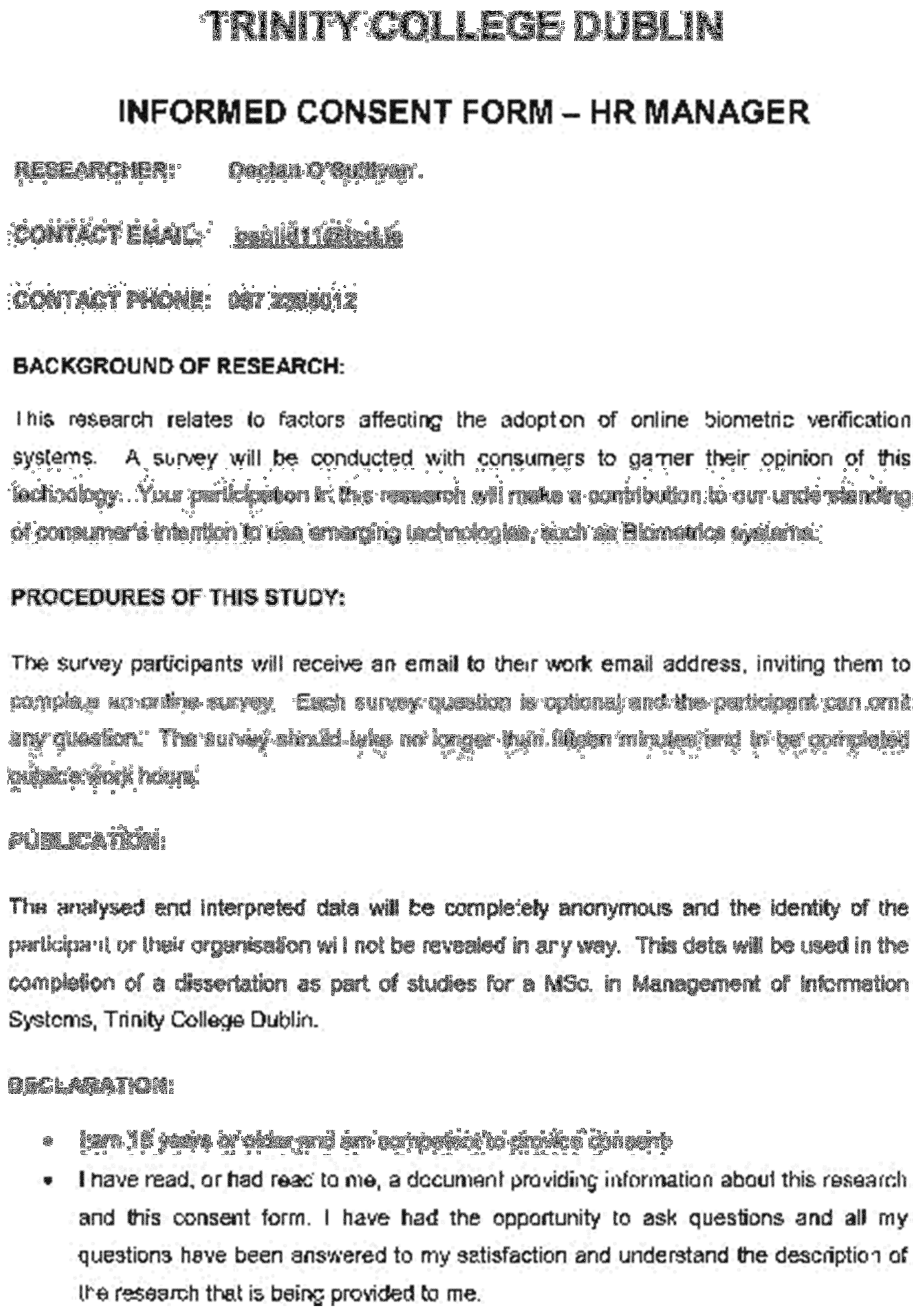
- A copy of the email that I would like to send to the survey participants. This email contains a link to the online survey;
- An information sheet for survey participants, which explains the background to the research question, the procedure, important notes and what happens to the survey findings;
- A pdf that contains the survey questions, for you to review the content;
- An informed consent form.

If you approve my request to distribute the survey to my work colleagues, then could I ask you to sign the attached informed consent form and I will collect this from your office.

Should you have any questions please do not hesitate to contact me.

Kindest Regards,

Declan O'Sullivan



TRINITY COLLEGE DUBLIN

INFORMED CONSENT FORM – HR MANAGER

RESEARCHER: Declan O'Sullivan.

CONTACT EMAIL: osullid11@tcd.ie

CONTACT PHONE: 087 2388012

BACKGROUND OF RESEARCH:

This research relates to factors affecting the adopton of online biometric verification systems. A survey will be conducted with consumers to garner their opinion of this technology. Your participation in this research will make a contribution to our understanding of consumer's intention to use emerging technologies, such as Biometrics systems.

PROCEDURES OF THIS STUDY:

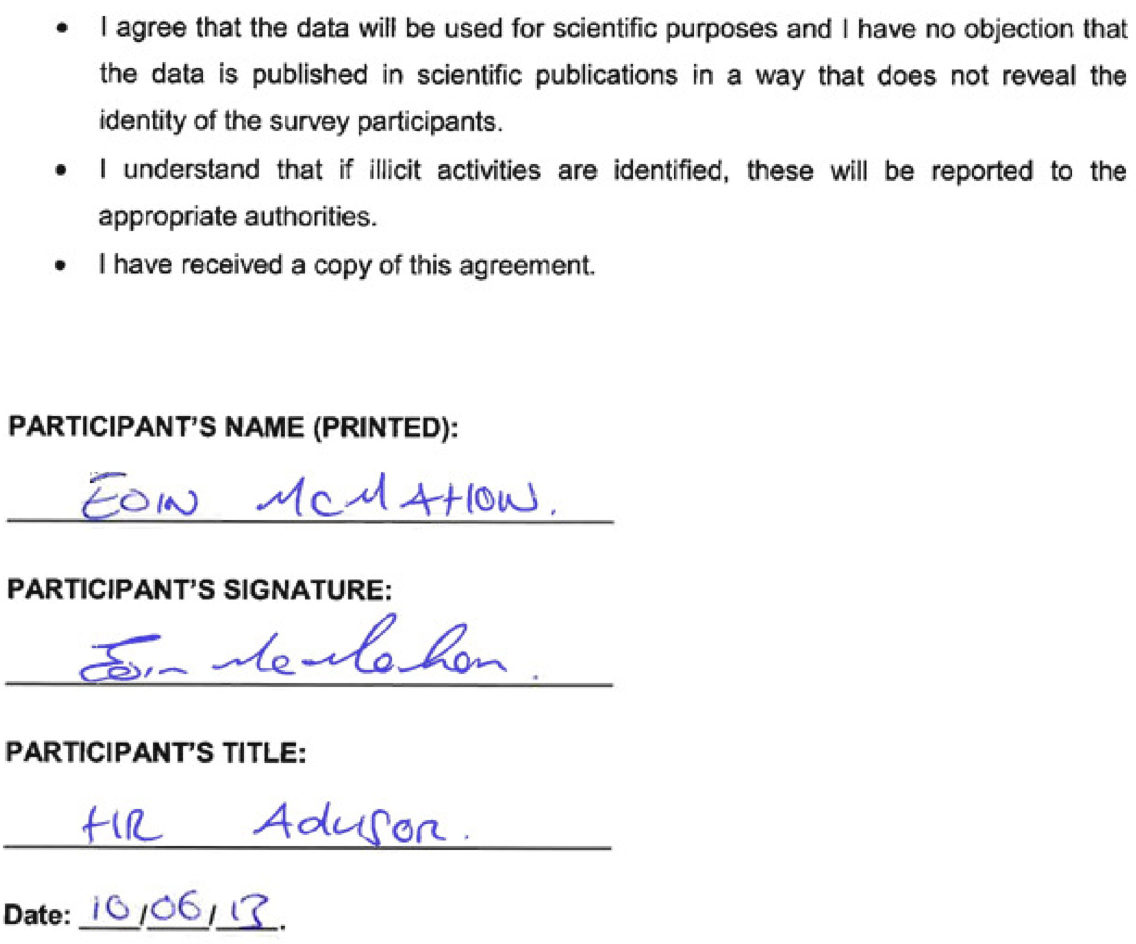
The survey participants will receive an email to their work email address, inviting them to complete an online survey. Each survey question is optional and the participant can omit any question. The survey should take no longer than fifteen minutes and to be completed outside work hours.

PUBLICATION:

The analysed end interpreted data will be completely anonymous and the identity of the participant or their organisation will not be revealed in any way. This data will be used in the completion of a dissertation as part of studies for a MSc. in Management of Information Systems, Trinity College Dublin.

DECLARATION:

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.



- I agree that the data will be used for scientific purposes and I have no objection that the data is published in scientific publications in a way that does not reveal the identity of the survey participants.
- I understand that if illicit activities are identified, these will be reported to the appropriate authorities.
- I have received a copy of this agreement.

PARTICIPANT'S NAME (PRINTED):

EOIN MCMAHON.

PARTICIPANT'S SIGNATURE:

Eoin McMahon.

PARTICIPANT'S TITLE:

HR Advisor.

Date: 10/06/13.

Appendix B

*Note: Only some responses displayed here which includes selects statements from the qualitiative data.

Title of questionnaire: ***Factors affecting the adoption of online biometric verification systems to prevent online identity theft***

1. Do you accept the above declaration and agree to participate in this survey

2. How often do you purchase online?

3. Are you concerned about your privacy while you are using the internet?

Always 30.4% Most of the time 24.0%
About half of the time 12.0% Once in a while 32.0% Never 1.6%

4. Have you purchased goods or services online in the last 6 months?

5. Do you own a PC or tablet or Smartphone (tick as many as apply)?

6. Which of these three devices do you use most often to purchases items on the web?

7. Have you been a victim of online identity theft? * Note: Online Identity theft is where cybercriminals get access to an individual's personal information to impersonate them and commit fraud - examples are credit card fraud, applying for loans & credit cards in the individuals name, illegal bank transfers.

Yes 10.4% No 77.6% Don't Know 12.0%

8. Are you concerned about online identity theft?

Yes 90.4% No 9.6%

9. Do you have any knowledge of Online Biometric systems?

Expert 0.0% Good 5.6% Average 21.8% Basic 33.9% None 38.7%

10. Have you heard of Online Biometric verification systems prior to this study?

Yes 56.5% No 43.5%

11. Which of the following Biometric technologies would you prefer to use - order in rank of preference from 1 to 5, (with 1 being your first choice and 5 being your least favourite)

12. The introduction of online biometric verification security systems will...

	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree	Don't know
make it more difficult for cyber criminals to steal my identity	41.6% (52)	**51.2% (64)**	1.6% (2)	2.4% (3)	0.0% (0)	3.2% (4)
be the silver bullet in the fight against online criminal activity	6.4% (8)	**32.0% (40)**	27.2% (34)	19.2% (24)	7.2% (9)	8.0% (10)
make it near impossible for an imposter to be verified as the individual they are trying to impersonate	10.5% (13)	**46.0% (57)**	22.6% (28)	13.7% (17)	1.6% (2)	5.6% (7)
always verify me as the real user	14.4% (18)	**46.4% (58)**	25.6% (32)	9.6% (12)	0.0% (0)	4.0% (5)
result in further growth in online purchases as people will become more confident and secure in using credit card details online	12.8% (16)	**46.4% (58)**	26.4% (33)	10.4% (13)	0.8% (1)	3.2% (4)
sometimes result in preventing me from purchasing online due to an inaccurate verification reading	6.5% (8)	**59.7% (74)**	14.5% (18)	12.1% (15)	0.8% (1)	6.5% (8)
not offer complete security as cybercriminals will quickly find a way to bypass them	14.5% (18)	**37.1% (46)**	29.8% (37)	14.5% (18)	0.8% (1)	3.2% (4)

13. Storage of digitalised biometric data...?

	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree
is an invasion of an individuals privacy	12.1% (15)	**33.1% (41)**	29.0% (36)	25.0% (31)	0.8% (1)
could be used for other unintended purposes without my consent	27.2% (34)	**56.0% (70)**	12.0% (15)	4.8% (6)	0.0% (0)
could be stolen from a company's website and used to impersonate me to commit fraud	33.6% (42)	**52.0% (65)**	8.8% (11)	4.8% (6)	0.8% (1)
could be intercepted in transmission and copied for use by criminal gangs	22.4% (28)	**50.4% (63)**	16.0% (20)	10.4% (13)	0.8% (1)
security around the storage of biometric data is a concern for me and would prevent me from using online verification websites	16.8% (21)	25.6% (32)	**33.6% (42)**	22.4% (28)	1.6% (2)
is not secure enough for my liking, using my biometric data at time of purchasing to unlock an encrypted code is more secure	16.1% (20)	**41.1% (51)**	26.6% (33)	12.9% (16)	3.2% (4)

14. Use of Biometrics will require....

	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree
low level training as my current experience with online purchasing will make the transition easy	18.4%	**55.2%**	16.0%	9.6%	0.8%
no special knowledge to submit data for online biometric security verification checks	8.0%	**48.8%**	25.6%	17.6%	0.0%
that I understand how the biometric reader interacts with the online biometric security check before I will use it	17.6%	**51.2%**	19.2%	12.0%	0.0%
that the biometric readers are easy to use	34.7%	**43.5%**	17.7%	3.2%	0.8%

15. In order for me to use an online biometric security verification system, it would require..?

	Strongly Agree	Agree	Neutral	Disagree	Strongly disagree
low costs set up for me as an individual	**48.0%**	39.2%	8.0%	3.2%	1.6%
that the verification system has been in use for some time before I submit my digitalised biometric data	36.8%	**50.4%**	9.6%	3.2%	0.0%
a biometric reader app to be made readily available for the smartphone / tablet	33.9%	**43.5%**	16.9%	5.6%	0.0%

16. With regards to biometrics... ?

	Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly disagree**
in the future, I will only use websites to purchase goods/services that have online biometric security verification checks enabled	4.0%	19.2%	**37.6%**	34.4%	4.8%
i believe that websites that enable online biometric security checks are doing so to protect their customers from identity theft	15.2%	**68.8%**	13.6%	2.4%	0.0%
i will only use biometric technology if I get positive feedback from family and Friends?	5.6%	**37.1%**	26.6%	27.4%	3.2%
i would avoid using a website					

that requests online biometric Security verification checks	0.8%	8.0%	30.4%	**50.4%**	10.4%

17. In order of preference, rank which security offering you would feel more secure with when purchasing online from 1 to 6 (With 1 being your first preference and 6 your least favourite) * Note: A digital certificate is an electronic "credit card" that establishes your credentials when doing transaction online. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Biometric Encryption identifies an individual solely by using his/her digitalised body characteristic to unlock an encrypted security code. The digitalised data is not stored anywhere and is discarded after use.

(Result: Biometrics and Pin number the best average rating at 2.24; Userid and Password had the lowest at 4.92)

	1	**2**	**3**	**4**	**5**	**6**	**Rating Average**
Biometrics(fingerprinting, iris recognition, voice recognition, face recognition) and Pin number	**44.4%**	23.4 %	12.1 %	8.1%	8.1%	4.0%	2.24
Userid and Password protection	4.0%	4.0%	9.7%	10.5 %	21.8%	**50.0%**	4.92
Userid, Password and Pin number protection	14.5%	12.1 %	12.9 %	21.8 %	**33.9%**	4.8%	3.63
Biometrics(fingerprinting, iris recognition, voice recognition, face	3.2%	**32.3 %**	29.0 %	15.3 %	11.3%	8.9%	3.26

recognition)							
Digital certification	9.7%	11.3%	12.9%	**27.4%**	14.5%	24.2%	3.98
Biometric Encryption	**24.2%**	16.9%	23.4%	16.9%	10.5%	8.1%	2.97

18. What type of information would you like to receive before starting to use biometric identification?

73	Data supporting the security of biometric ID use.
74	Full disclosure of what biometric identification would be stored. For how long would it be stored. Who would have access to it. What security protocols are in place. Would the biometric identification information be stored indefinitely or be erased after a certain period of inactivity as part of a security measure.
75	Full information regarding storage procedures of biometric data and legal documents relating to what procedures and recompense facilities there are in event of data loss of theft.

19. What factors would prevent you as a user from using biometrics as an identification verification system?

20	Which firms have started using it as a primary identification verification system. For example, if Google, Amazon, and the gov't didn't adopt it, I would be hesitant to use it with other firms. The big flagship firms would have to use biometrics before I would buy into it as a whole.
21	Concern about the security of its storage
22	If someone steals my password, I can change it. If someone steals my biometric details, I would feel it is a massive invasion of privacy and could lead to serious breach of security and identity theft.
23	risk that the information stored by the company will be stolen
88	Since biometric data is static once intercepted it can be used to impersonate a user for life. Key cards such as the RSA key card commonly used for VPN access seems like a more secure as it is a non-static key and can be changed if and when it or the algorithm underlying it is compromised.

20. Are you concerned that if you use your credit card to buy something on the internet your credit card number will be intercepted by someone else?

Very Concerned 14.4% Concerned 52.8%

Neither Concerned or Unconcerned 15.2% Not really concerned 17.6%

Not concerned at all 0.0%

21. Are you concerned that if you use your credit card to buy something on the internet your card will be mischarged?

22. Do you have an account on a social networking website (e.g. Facebook or Twitter)?

Yes 91.2% No 8.8%

23. if yes to q22, to what level have you restricted access to your personal information?

Close Friends 34.2% Friends 57.9% Public 6.1%
Network 0.0% Don't know 1.8%

24. Have you ever switched off security settings to improve performance of Internet Browsing?

25. Do you have security software installed on your devices (tick as many as apply)?

PC 94.1% Netbook13.6% Tablet 14.4%
Mobile 30.5% All of the above 6.8%

26. Do you allow for automatic security updates for ...?

Operating systems

Application software

Security software

27. Do you read a website's privacy policy before you register your information?

Always 4.0% Most of the time 15.3% About half of the time 11.3%

Once in a while 31.5% Never 37.9%

28. Do you look for a privacy certification on a website before you register your Information?

Always 11.2% Most of the time 14.4% About half of the time14.4%
Once in a while 24.8% Never 35.2%

29. Do you only register for websites that have a privacy policy?

Yes 18.4% No 49.6% Don't know 32.0%

30. How often do security concerns prevent you from purchasing online?

Always 4.8% Most of the time 6.5% About half the time12.9%

Once in a while 67.7% Never 8.1%

31. Do you check to see if the network is secure before you purchase online?

Always 38.4% Most of the time 17.6% About half of the time 7.2%

Once in a while 12.0% Never 24.8%

32. Are you concerned that you are asked for too much personal information when you register or make online purchases?

Yes 64.5% No 35.5%

33. How confident are you that your personal information is kept confidential when buying items online?

Extremely confident 0.8% Very confident 8.9% Moderately confident 46.0%
Slightly confident 23.4% Not at all confident 21.0%

34. Where a website offers a third party service such as Paypal to transact online - do you avail of this?

35. What are your biggest concerns about purchasing online?

54	Potentially that CC details could be taken. or too much information is requested
55	Up until recently all my experiences were positive. However, my credit card was recently defrauded and about €2,000 of purchases were put through. This experience has made me be cautious and to be watchful of online purchasing fraud
56	Storage of information after I have submitted - interception in transit is pretty unlikely, much more likely hackers will try to access information stored on a inadequately secured server.
57	- identity theft - misuse of my credit card details - the purchase to never arrive to my front door..
58	Credit card details being divulged.
63	Credit card fraud.
64	My information being passed onto a third party and getting continuous emails as a result. If it happens with my personal details then it could also happen with credit card details

36. Are you concerned about online organisations not being who they claim they are?

Always 12.0% Most of the time 12.0% About half of the time 16.8%

Once in a while 54.4% Never 4.8%

37. Are you concerned about people you do not know obtaining personal information about you from your online activities?

Yes 89.6% No 10.4%

38. Have you ever received phishing email messages? *Phishing emails are sent by cybercriminals seeking your personal details, - it could contain fake links to popular websites where you are asked to enter your personal information to retain a service. The fake threat is that if you don't you could be disconnected, or something as simple as an email requesting your bank details so that they can transfer funds to you.

39. Do you delete cookies after Internet browsing?

40. What is your gender?

41. Which category below includes your age?

42. Are you happy to submit your answers