Dissertations                                                                                 School of Computing

2012

# Biometric Alternatives to CAPTCHA: Exploring Accessible Interface Options

Anita Foley
*Technological University Dublin*

# Biometric Alternatives to CAPTCHA: Exploring Accessible Interface Options



**Anita Foley**

A dissertation submitted in partial fulfilment of the requirements of

Dublin Institute of Technology for the degree of

M.Sc. in Computing (Assistive Technology)

**July 2012**

I certify that this dissertation which I now submit for examination for the award of MSc in Computing (Assistive Technology), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the test of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute's guidelines for ethics in research.

*Signed:* _____

*Date:*          *16th July 2012*

# ABSTRACT

In the computing domain the relationship between accessibility and security is a complex and evolving one; accessibility attempts to ensure that as wide a range of individuals as possible are granted access to systems, whereas security attempts to restrict access only to individuals who are entitled to access those systems. A key security concern is to determine whether or not the system is being accessed by a software agent or a real human being, and a number of approaches have been developed to determine the answer to this question. This issue has been discussed throughout the history of computer science and its roots can be traced back to Alan Turing's 1950 paper "Computing Machinery and Intelligence" from which the so-called "Turing Test" derives its name.

A very common approach to this question is the CAPTCHA (the "Completely Automated Public Turing test to tell Computers and Humans Apart"), which requires a human being to perform a visual test, typically recognizing alphanumeric characters that are obscured or warped in some way to make Optical Character Recognition (OCR) difficult. This seemingly effective approach highlights the essential tension between security and accessibility, since it provides significant challenges to rely on a visual character recognition test when considering users with visual impairments or learning difficulties.

In this work, an accessible biometric alternative to the CAPTCHA user interface is proposed. In the event of a single sign-on biometric recognition system, the interface developed has the potential to exploit the capabilities of the iPad platform to provide universal access. The proposed interface, BioScope, is implemented using accessible development and evaluation methodologies to ensure universal and inclusive design. Following implementation, the interface is evaluated and compared with CAPTCHA using a series of surveys, questionnaires and prototype experiments with the aim of determining if BioScope's approach is a viable accessible alternative to the CAPTCHA user interface.

Keywords: *Accessibility, CAPTCHA, Biometrics, Assistive Technology, Universal Design.*

## ACKNOWLEDGEMENTS

I'd like to begin with thanking my supervisor, Ciarán O'Leary, for his guidance, support and enthusiasm throughout this process. This dissertation has meant more to me than any other item of work I have completed thus far in my life and for that I am eternally grateful.

I'd also like to thank my family and friends for their support and patience over the past 2 years. Their encouragement never went unnoticed and without it none of this would have been possible.

Finally, I'd like to thank my boyfriend and partner in crime, David, for encouraging and motivating me each and every day. Your positive attitude and outlook on life is a constant inspiration to me that I would truly be lost without.

# TABLE OF CONTENTS

# TABLE OF FIGURES

# TABLE OF TABLES

# 1   INTRODUCTION

## 1.1  Background to Research

It is estimated that 75.8% of all email exchange on the Internet is sent by spam accounts (Symantec 2011). Of this 75.8%, 82.2% of these spam accounts are generated and maintained by malicious automated systems called bots (Symantec 2011). These spam accounts are not only a nuisance to email service users, but are also a costly waste of the resources belonging to the service providers (Stone-Gross et al. 2011).

A solution to this spam problem is to prevent bots from creating these nuisance email accounts. Many email service providers like Yahoo, Microsoft and Google use a CAPTCHA system to prevent this malicious email account generation. A CAPTCHA (**C**ompletely **A**utomated **P**ublic **T**uring Test to **T**ell **C**omputers and **H**umans **A**part) is an automated system that is designed to tell if a computer user is a human being or a bot (L. von Ahn et al. 2002). This system was developed by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford in 2000 (Pinar Saygin et al. 2000).

A CAPTCHA poses the user with a randomly generated test. The user is shown a sequence of distorted images, numbers or shapes and is then asked to type in that sequence of characters into a text field, illustrated in Figure 1. This test is designed so that humans can pass it easily but that computer systems, like bots, cannot. There are many different types of CAPTCHA tests. These include text-based tests, image based tests and audio based tests.



**Figure 1: Example of Google CAPTCHA**

The alphanumeric characters presented by a CAPTCHA are not always easy for humans to identify (Yan & El Ahmad 2008b). Considering this, there are many accessibility and usability issues relating to the use of CAPTCHA for users with visual impairments or learning difficulties. The W3C, who regulate the web, propose a single sign-on biometric recognition system as a potential solution (W3C 2005). A single sign-on system allows a user to access multiple online resources using one account, as illustrated in Figure 2.
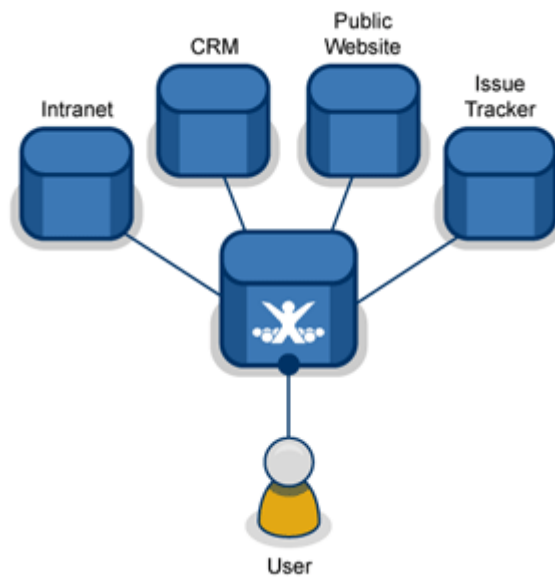


**Figure 2: Single Sign-on Architecture (Atlassian 2012)**

## *1.2 Research Aim*

This research aims to establish an accessible alternative to CAPTCHA using design and testing methodologies that promote usability and accessibility. Using these processes we introduce BioScope, an interface to a single sign on system which can potentially serve as an alternative to CAPTCHA, as illustrated in Figure 3. This system captures user's biometric data in an accessible and usable manner exploiting in full the capabilities of the iPad tablet, including the inbuilt microphone to capture human voice data, inbuilt camera to capture face information and its multi-touch screen to capture a person's handwriting. This information is stored on the iPad and provided to a biometric recognition system on a remote server to identify if the user is a human being or a bot (the implementation of which is outside the scope of this work).
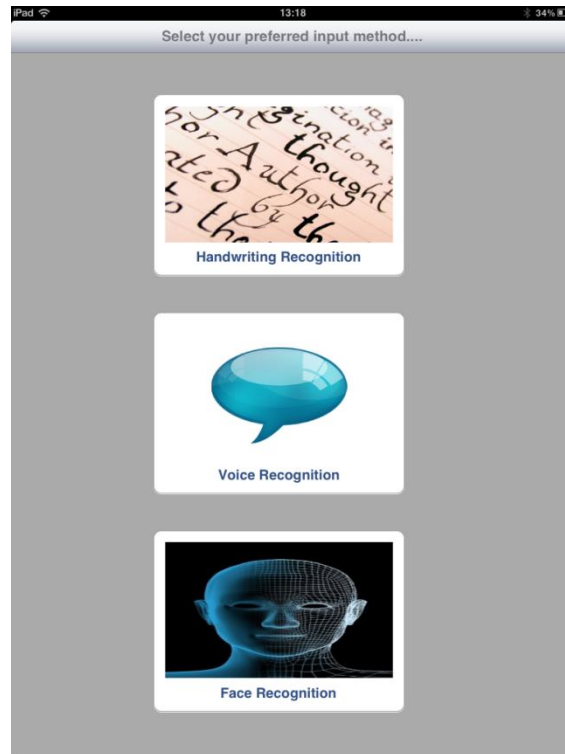
**Figure 3: BioScope's Biometric Selection Screen**

## *1.3 Research Objectives*

The main objectives for this project are as follows:

1. Literature Review:
    a. Research the area of accessibility in the domain of information technology.
    b. Investigate and examine CAPTCHA alternatives that are currently available to Internet users.
    c. Investigate and evaluate different biometric recognition systems in terms of current usage and security.
2. Explore biometric recognition systems and their acceptability in the public domain using a survey.
3. Explore CAPTCHAs usage and user satisfaction in the public domain using a survey.
4. Propose a testing methodology that aims to promote a high level of accessibility and usability in software user interfaces.

5. Develop and test an interface of an accessible CAPTCHA alternative exploiting the biometric capabilities of the iPad platform:
   a. Gathering requirements.
   b. Design the software's user interface.
   c. Prototyping and implementing the software.
   d. Testing the software on users with a wide range of abilities and skills.
6. Evaluate and Analyse Results :
   a. Evaluate quantitative and qualitative data collected during testing.
   b. Compare the developed software to the original CAPTCHA process.
7. Make recommendations for future research in the area.

## *1.4  Research Methodology*

In this work, the literature review provides an understanding of CAPTCHA, accessibility and biometrics.

The different variations of CAPTCHA and their alternatives are investigated using qualitative and quantitative data in the form of surveys, questionnaires and user testing. This provides an overview of the strengths and weaknesses of CAPTCHA, and in particular identifies the issues that people, including those with disabilities, face when using a CAPTCHA system.

Various biometric recognition methods are evaluated, as outlined in the literature review, in terms of these accessibility and public perception using universal design techniques, surveys and interviews.

This research regarding CAPTCHA and biometrics is used to develop BioScope, an accessible biometric alternative to CAPTCHA. For the experiment, testers are asked to use the BioScope application and a pre-existing text/audio based reCAPTCHA application. During this testing, time results and failure rate quantitative data is recorded. Qualitative data relating to the user's frustration and comfort levels are also recorded using a user satisfaction questionnaire.

The results from this testing is evaluated to determine if, and to what degree, the BioScope application is more usable and accessible than the reCAPTCHA system.

## *1.5 Project Deliverables*

1. A literature regarding Accessibility, biometric recognition and CAPTCHA.
2. The user interface of the accessible biometric CAPTCHA alternative (BioScope).
3. CAPTCHA usage and user satisfaction survey results.
4. CAPTCHA usage and user satisfaction interview transcripts.
5. Biometric public acceptance survey results.
6. Biometric public acceptance interview transcripts.
7. Evaluation of BioScope.
   a. Comparisons of time results collected during CAPTCHA and BioScope testing.
   b. Comparisons of error rates collected during CAPTCHA and BioScope testing.
   c. Comparisons of user satisfaction questionnaire results for both CAPTCHA and BioScope.
8. Recommendations made for future work in the area.

## *1.6 Resources*

For the purpose of research the following resources are required:

1. Access to 10 testers with varying abilities, skills and disabilities, as illustrated in Table 1.

**Table 1: Tester Resources**

|   | **Tester Identification** | **Tester Profile** |
|---|---|---|
| 1 | **Tester A** | Computer Novice |
| 2 | **Tester B** | Computer Novice |
| 3 | **Tester C** | Computer Expert<br>Colour Vision Limitations |
| 4 | **Tester D** | Computer Intermediate |

| 5 | **Tester E** | Computer Expert |
| | | English is not first language |
| 6 | **Tester F** | Computer Expert |
| | | Dyslexic |
| 7 | **Tester G** | Computer Intermediate |
| 8 | **Tester H** | Computer Expert |
| | | Broken Elbow |
| 9 | **Tester I** | Computer Intermediate |
| | | Arthritis |
| 10 | **Tester J** | Computer Expert |
| | | Blind |

2.  Access to a Mac development environment to develop the iPad software for the experiment.

3.  Access to online papers and journals to allow for the completion of the literature review for this project.

4.  Access to online survey software to conduct surveys regarding CAPTCHA and biometrics usage.

## 1.7  Scope and Limitations

The primary focus of this research is to establish a biometric single sign-on alternative to CAPTCHA, called BioScope, using development and testing methodologies that promoted universal and inclusive design. The aim is to demonstrate that by using these methodologies the resulting BioScope system is more accessible and usable than its CAPTCHA counterpart.

The implementation of the BioScope system is limited to the development of the user interface and the tasks involved with capturing the biometric data, highlighted in Figure 4. This system does not provide any biometric recognition processes nor does it send the captured biometric information to a remote server for analysis or user single sign-on account generation.
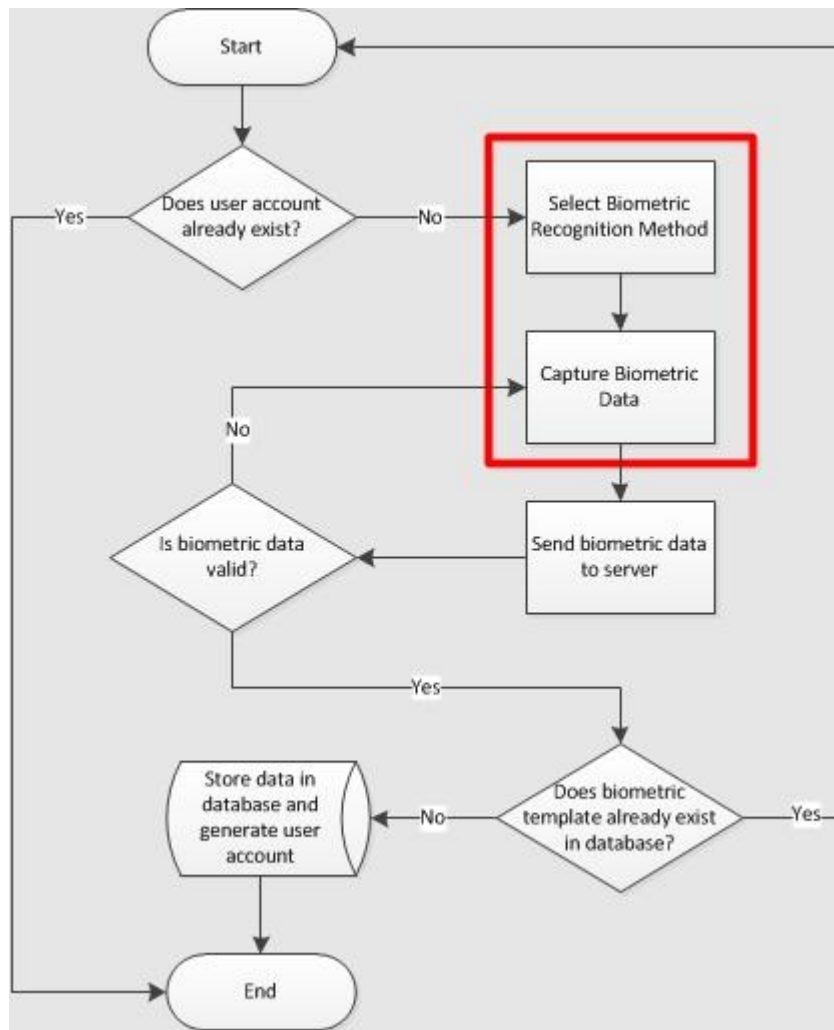
**Figure 4: Flowchart of BioScope**

## 1.8 Organisation of Dissertation

This project is organised into the following chapters:

- Chapter 2: Accessibility

  This chapter provides an overview of the area of accessibility. It identifies the common issues faced by people with disabilities and discusses how assistive technologies can be used to resolve these issues. This chapter also outlines the various design tools and methodologies that promote accessibility and usability in both the physical and software world.

- Chapter 3: CAPTCHA

  This chapter investigates the various types of CAPTCHA that are available to Internet users today. It establishes the strengths and weaknesses of these variations in terms of security, accessibility and usability.

- Chapter 4: Biometrics

  This chapter provides a summary in the domain of biometric recognition. This includes an overview of different biometric recognition systems including an investigation of their current usage in the information technology sector and the security issues that these systems face.

- Chapter 5: Methodology

  This chapter outlines the various methodologies used in the context of the experiment. This includes the methodology used for the survey design, BioScope's development methodology and the final testing process.

- Chapter 6: Experiment

  This chapter discusses the experiment that was conducted as part of this project. This includes a description of how the design and testing methodologies, established in Chapter 5, were incorporated into the development process of BioScope.

- Chapter 7: Results and Analysis

  This chapter analyses the qualitative and quantitative data collected as part of the experiment. These results are compared and contrasted with the aim of determining if the BioScope application is more usable and accessible than CAPTCHA.

- Chapter 9: Conclusions

  This chapter presents a summary of the project and discusses the final outcomes of the experiment. It provides conclusions regarding this work and recommends details of future research that could be conducted in this area.

# 2   ACCESSIBILITY

## 2.1 *Introduction*

There are many definitions used for accessibility, usability and disability. This chapter explores these definitions in order to gain an understanding of the types of disabilities that people can have, the issues that they face on a day to day basis and how the use of assistive technologies can help to resolve these issues.

In the domain of information technology, the use of assistive technologies and their capabilities must be understood when designing and implementing computer software. This chapter outlines the various design principles, guidelines and motivations that encourage designers and developers to create accessible and usable computer user interface. When testing and evaluating these user interfaces, many different tools and methodologies can be used. This chapter provides an overview of these tools and methods, in particular focusing on the idea of *usable accessibility* which incorporates the accessibility philosophy of inclusive and universal design together with pre-existing usability measurements.

## 2.2 *Defining Accessibility and Usability*

The terms accessibility and usability are often used interchangeably in the area of information technology, however, these two terms do not share the same meaning (Fänge & Iwarsson 2003).

The ISO defines Usability as,

> "*The **effectiveness**, **efficiency** and **satisfaction** with which specified users achieve specified goals in particular environments*".

Effectiveness relates to how accurately a task can be completed by a user. The efficiency relates to the expenditure of time and resources needed to complete a specified task. Satisfaction is determined by how comfortable and acceptable the task experience is to the user (W3C 2002).

The definition of Accessibility is defined by W3C in terms of the Web as,

> "*Web accessibility means that people with disabilities can use the Web... More specifically, Web accessibility means that people with disabilities can perceive, understand, navigate, and interact with the Web*" (WAI 2011).

These definitions suggest that usability is determined by how well a specific user group can complete a task, whereas accessibility is determined by how well a diverse group of users can complete a task. Considering this, Petrie and Kheir suggests that the definition of accessibility should simply extend the pre-existing definition of usability.

> "*an [accessible] product/website can be used by specified users with specified disabilities to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use*" (Petrie & Kheir 2007).

This definition transform the term "*accessibility*" into the a new term of "*usability for people with disabilities*" or even "*usable accessibility*" (Di Blas et al. 2004). This definition continues to instil the concepts of usability, but also considers the various types of disabilities people can have and issues that they can face day to day.

## 2.3 Defining Disability

Disability can be defined using two separate definitions; the medical model definition and the social model definition.

The medical model is used by the World Health Organisation, who defines disability using three classifications; impairment, disability and handicap:

> "***Impairment***: Any loss or abnormality of psychological, physiological, or anatomical structure or function. ***Disability***: Any restriction or lack (resulting from impairment) of ability to perform an activity in the manner or within the range considered normal for a human being. ***Handicap***: A disadvantage for a given individual, resulting from an impairment or disability, that limits or

*prevents fulfilment of a role that is normal, depending on age, sex, social or cultural factors for that individual"* (World Health Organization 2001)

This definition of disability focuses on the clinical diagnosis of the disability (Brisenden 1986). The definition can cause a partial and inhibiting view of people with disabilities as it suggests that a person's functional or structural limitations are what cause the disability (Brisenden 1986). The medical model focuses on attempting to treat or cure these limitations as a solution (Crow 2010).

In contrast, the social model definition of disability moves focus from the clinical diagnosis. The United Nations define disability using a social model:

*"a disability results from the interaction between persons with impairments, conditions, or illnesses and the environmental and attitudinal barriers they face. Such impairments, conditions, or illnesses may be permanent, temporary, intermittent, or imputed, and those that are physical, sensory, psychosocial, neurological, medical or intellectual"* (United Nations Enable 2004).

The social model suggests that environmental and social barriers are the root cause of disability rather than the person's physical or cognitive limitations (Crow 2010). The social model suggests that the cure to disability is not in treating a person's impairment, but to remove the social and environmental barriers. Removing these barriers allows people with disabilities to participate fully in society (Mulvany 2000). For example, a wheelchair user may have difficulty entering a building. The medical model views the person's inability to walk as the root cause of the disability. However, the social model suggests that the fact that no ramp is provided at the entrance to the building is what causes the disability and prevents the person from entering the building.

## 2.4 Impairments

While the definition of disability is still debated, the concept of impairment is not. Currently over a billion people in the world live with some form of structural or

functional impairment (WHO 2011). This includes individuals with visual impairments, physical impairments and learning difficulties.

## 2.4.1  Blind and Low Vision

285 million people are visually impaired worldwide (WHO 2012b). 39 million of these are fully blind and 246 million suffer from low vision. Approximately 90% of all blind or low vision people live in developing countries. 80% of all visual impairment can be prevented or cured (WHO 2012b). Blindness is defined by the World Health Organisation (WHO) as a visual acuity of less than 3/60 or a corresponding visual field loss in the better eye with best possible correction. Low vision is defined as visual acuity of less than 6/18 but equal to or better than 3/60 in the better eye with best possible correction (WHO 2012b).

Uncorrected refractive errors are the leading cause of low vision (43%) in the world. This includes myopia (short-sightedness) and hyperopia (long-sightedness). Refractive errors in the eyes can be correct by wearing prescription lenses. The leading causes of blindness in the world are cataract, trachoma and glaucoma (Thylefors et al. 1995).

33% of global blindness is cause by Cataracts (WHO 2012b). Cataracts cause the lens of the eye to become cloudy. This clouding prevents sufficient light entering the eye which leads to perceived colour distortion and blurred vision (NCBI 2012a), as illustrate in Figure 5. Cataracts is both curable and operable, by using eye drops in less severe cases or performing a eye lens replacement surgery in more extreme cases (Brian & Taylor 2001) .
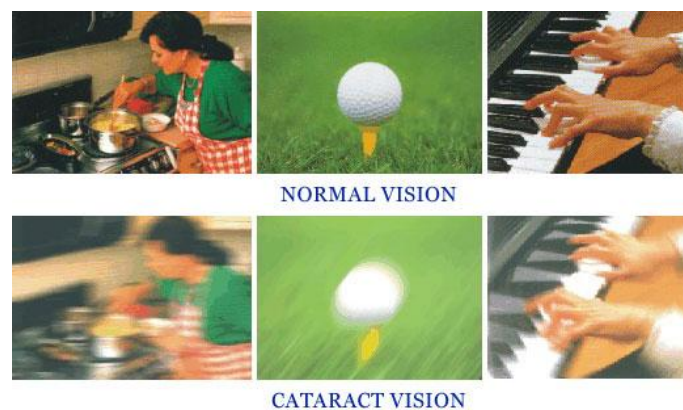


**Figure 5: Vision with Cataracts (Metwest Eye Centre 2012)**

Glaucoma is an eye condition that causes a build up of fluid around the optic nerve. This fluid damages the optic nerve by putting an increased amount of pressure on it (NCBI 2012b). This permanent damage leads to a loss of peripheral vision and over time can lead to complete vision loss (Cense et al. 2002), as illustrated in Figure 6. It is estimated that 2% of global blindness is caused by Glaucoma (WHO 2012b).



**Figure 6: Vision with Glaucoma (C.L.Gupta Eye Institute 2009)**

Trachoma causes 15% of the world's blindness (Thylefors et al. 1995). Trachoma is caused by an ocular infection that leads to chronic inflammation of the eyelids. This inflammation produces scarring on the inside of the eyelid which can cause the eye lid to turn in on itself causing the eyelashes to damage the cornea of the eye (Mariotti et al. 2009).

2.4.2 Learning Disabilities

A learning disability is defined as,

> *"a significantly reduced ability to understand new or complex information, to learn new skills (impaired intelligence), reduced ability to cope independently (impaired social functioning) which start before adulthood, with lasting effect on development"* (Whitaker & Porter 2002).

A common type of learning disability is dyslexia. Dyslexia is a specific learning disability which causes difficulty in learning to read, write and spell correctly. 8 to 10% of the world's population suffer from dyslexia. Research suggests that dyslexia can be inherited (S. D. Smith et al. 1998). It is estimated that if a parent has dyslexia, there is a 40-60% chance that their child will also have dyslexia (HSE 2012).

The exact causes of dyslexia are still unknown (DAI 2012). Many of the research conducted in this area supports the theory that a phonological processing impairment is the root cause (HSE 2012). A phonological processing impairment occurs when a person has difficulty matching spoken language to written language. Brain activity imaging shows that people with dyslexia do not use the same brain regions when reading. In particular non-dyslexic readers use the left hemisphere, often considered the language side, far more than dyslexic readers (Paulesu et al. 2001).
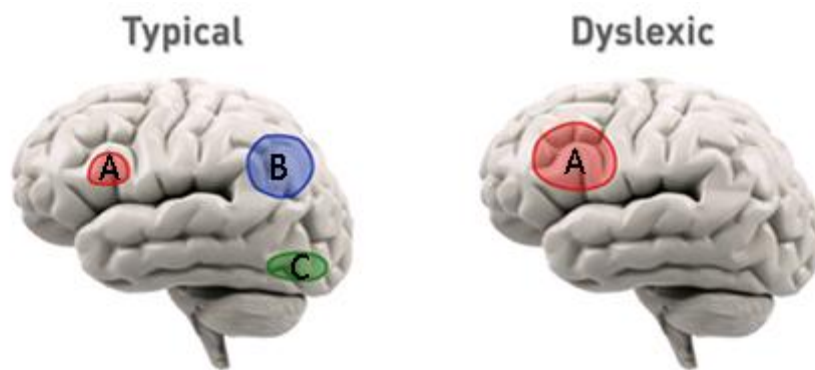


**Figure 7: Dyslexic Brain Activity (Doidge 2012)**

There are three areas of the brain found in the left hemisphere that differ in activity between a dyslexic reader and a non-dyslexic reader (Duara et al. 1991), as illustrated in Figure 7:

- **Broca's area (A):** Is involved in producing written words. Dyslexic readers use a larger portion of this area than non-dyslexic readers.
- **Parietotemporal region (B):** Is involved in analysing written words. Commonly this region of the brain is not used by dyslexic readers.

- **Occipitotemproal region (C):** Is involved in identifying written words. This region of the brain is often not used by dyslexic readers.

## 2.4.3 Physical Disabilities

A physical disability is a sensory motor dysfunction that causes an individual difficulty with motor activities like walking and lifting heavy objects (Jette & Branch 1981). The term physical disability is a broad category that represents a large number of different limb and dexterity disabilities. These disabilities can range from an in-born or acquired difficulty caused by illness or injury. Two common physical disabilities are Multiple Sclerosis and Arthritis.

Multiple Sclerosis (MS) is one of the most common diseases of the brain and spinal cord (central nervous system) and cause of physical disabilities in young adults worldwide (WHO 2008). The impairments caused by MS can range from mild to severe impairments. Some MS suffers can experience little physical difficulties during their lifetime, however, 60% of individuals with MS are unable to walk 20 years after onset (WHO 2008). In the body of an MS sufferer, the protective layer that surrounds the body's nervous system, called myelin, breaks down or becomes scarred, as illustrated in Figure 8. This causes a distortion of the electrical messages coming from the brain resulting in loss of feeling and movement in the body's limbs (MS Ireland 2011).
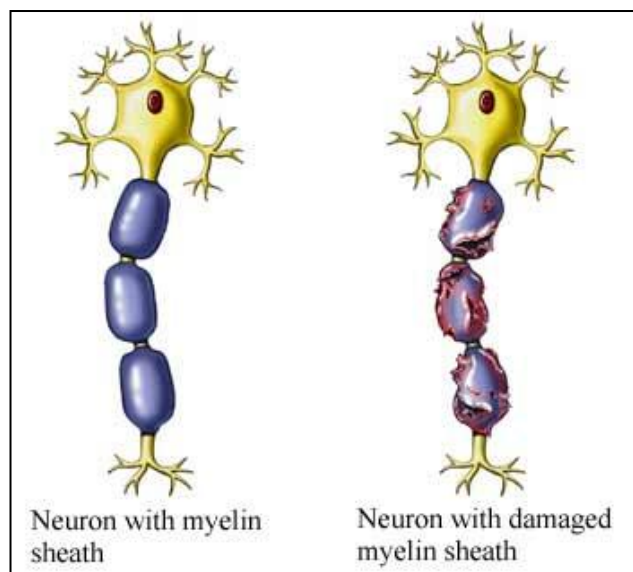


**Figure 8: Myelin Damage (EmpowHer 2012)**

Another common physical disability is Arthritis. Arthritis is an inflammation of joints in an individual's body. This inflammation causes pain, fatigue and long term damage to the joints resulting in deformity. There are over 100 types of arthritis, two of the most common being Rheumatoid Arthritis and Osteoarthritis (Arthritis Ireland 2012). Rheumatoid Arthritis (RA) is a chronic systemic disease that affects the joints, tendons, muscles and connective tissues in the body. The inflammation of the joints in RA is caused when an individual's own immune system attacks the joints and organs in the body instead of protecting them. The reasons for this reaction are still unknown (Arthritis Ireland 2012). Within 10 years of the onset of RA, at least 50% of sufferers will be unable to work a full-time job (WHO 2012a). Osteoarthritis (OA) is a degenerative disease caused by trauma, age or infection in a joint. It is estimated that 9.6% or men and 18% of women over the age of 60 suffer from OA (WHO 2012a).

## 2.5 Assistive Technologies

The International Standard's Office defines assistive technology as,

> "*any product, instrument, equipment or technical system used by a disabled or elderly person, made specially or existing on the market, aimed to prevent, compensate, relieve or neutralise the deficiency, the inability or the handicap*" (World Health Organization 2001) .

This means that any technology, whether low tech or high tech, that helps a disabled user is deemed as an assistive technology. Assistive technology enables people with disabilities to participate in society as contributing community members. These technologies can also allow people to achieve optimal functionality and independence assuming that the assistive technology fully meets the needs of the user in a given context (Reimer-Reiss 2000).

### 2.5.1 Braille

Braille is a haptic reading and writing system used by blind and visually impaired people. It was originally designed by Louis Braille in the early 19th century to help blind children to read (Büchel 1998). The system uses an arrangement of raised dots or

absent dots on paper, allowing a person to move their finger over these dots and interrupt each Braille character (Lévesque et al. 2005). Each Braille character represents a letter in the alphabet, as illustrate in Figure 9.
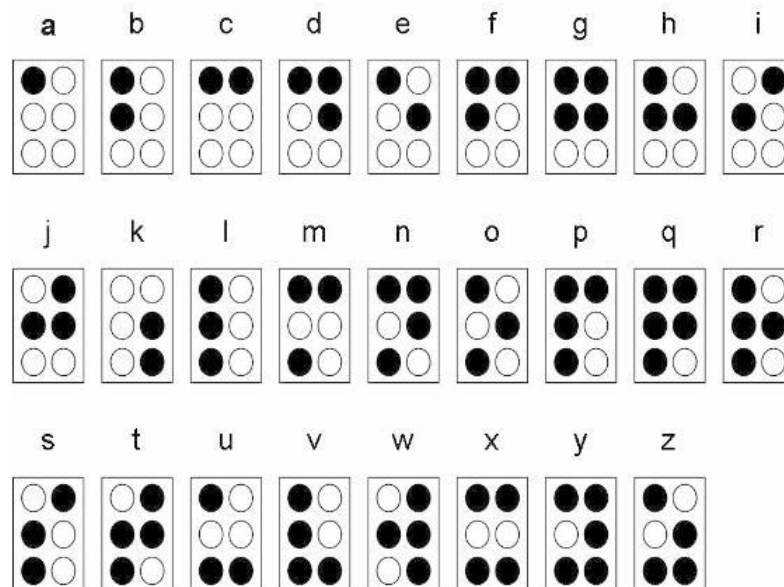


**Figure 9: Braille Alphabet (SFA 2012)**

Traditionally Braille is printed on embossed paper, but with the use of computers, text to Braille systems can be used through the use of a refreshable Braille display, as illustrated in Figure 10. A refreshable Braille display represents text on a computer screen in a Braille format using a system of pins that automatically rise and fall with each on-screen letter. Refreshable Braille displays remain one of the most common systems used by blind and low vision users to access information on computer systems (Lévesque et al. 2005).



**Figure 10: Refreshable Braille Display (Cantor Access Inc. 2012)**

## 2.5.2 Screen Reader

Another common assistive technology that blind and low vision people use to interact with information on a computer screen is a screen reader. A screen reader is a text to speech system that reads out information that is represented on a computer screen. Using a variety of shortcut keyboard keys, a user can navigate through the user interface and read all text available on the screen. Users can also type text using the computer keyboard, and the screen reader will transform the letters they type into a speech representation.

The first screen reader *IBM Screen Reader* was invented in 1986 by Jim Thatcher (Cooke 2004) . This screen reader was designed to read out the text that appeared on a command line in DOS. Following the shift from using DOS to a more graphical interface, *IBM Screen Reader/2* was released in 1988. *IBM Screen Reader/2* was the first screen reader designed to be used with graphical user interfaces (Thatcher 1994). This screen reader was controlled using the number keys on a computer keyboard (Asakawa 2005).

A screen reader works by creating an off-screen buffer that contains all the information that is available on the computer monitor (Blenkhorn & Evans 2000). It is this information buffer that is then read out to the user. The screen reader uses system hooks to capture the user's keyboard input, thus enabling the user to control the screen reader using keystrokes. Four of the most common screen readers used today are *JAWS* by Freedom Scientific (74%), *Window-Eyes* (23%), an open source screen reader called *NVDA* (8%) and the inbuilt Apple screen reader *VoiceOver* (6%) (J. Smith 2009).

## 2.5.3 Switch Access

Switch access devices are used by people with physical disabilities to navigate through and interact with computer user interfaces using a single control. They replace the need for keyboard and mouse usage which individuals with physical disabilities can find it difficult to use due to the large movement and dexterity required (Assist Ireland 2012).

There are a range of switch devices available to computer users. They come in a variety of sizes and can have different interaction styles (using hands or feet) to meet the needs of an individual user, as illustrated in Figure 11.

A switch device operates by a user selecting a control on a user interface using either an automatic, directed or step scanning function (Davies et al. 2010). An automatic scanning function automatically focuses on and highlights the various controls on a user interface in a sequenced manner. When a control that the user wants to activate is highlighted, the user hits the switch device in order to select it. A step scanning function works in similar manner to that of the automatic scanning function, with the difference being that the scanning is manually controlled by a user using a two switch access devices; one for controlling the scanning mechanism and the other for selecting the control. Directed scanning is controlled by a user by holding down the switch control and when the desired user interface control is highlighted the user releases the switch in order to interact with the button.



**Figure 11: Switch Access Devices (Assist IT 2012)**

## 2.5.4 Speech Synthesis

Individuals with learning disabilities like dyslexia can find it difficult to read and write information displayed in books and on a computer screen (Faundez-Zanuy 2005). Speech synthesis software can assist these individuals using two approaches; Text to speech and Speech to text.

Text to speech software acts as a reading assistant that provides speech output representing the information displayed on the computer screen or in a book, similar to how a screen reader works. Books are scanned in using Optical Character Recognition (OCR) software and the information is then transformed to speech output.

Speech to text software acts as a writing assistant for individuals by transforming speech inputted through a microphone into a textual representation on the computer screen.

## *2.6 Accessible Design*

Assistive technologies can only function correctly if the computer user interface that it is interacting with is designed in an accessible manner. This places ownership on the interface designers and developers to enable assistive technologies to interact correctly with their user interfaces to ensure that the needs of people with disabilities are met. To assist these designer and developers with this task there are a number of usability and accessibility design methodologies, guidelines and principles.

### 2.6.1 Universal Design

In the mid 1980s, Ron Mace (an architect who was a wheelchair user) coined the term Universal Design (Thompson et al. 2002). Mace held a view that all elements in the built environment should be designed universally for all users whether disabled or not. This broke away from previous mindsets that felt inaccessible built environments were acceptable as long as special purposed alternatives were provided (Thompson et al. 2002). Mace believed that these alternatives stigmatized the people who used them.

Using Mace's concepts, Universal Design was defined by the Center of Universal Design in 1997 as *"the design of products and environments to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design"* (Center for Universal Design 2008) .

From this definition the Center for Universal Design compiled the *Principles of Universal Design*:
1. Equitable Use

2. Flexibility in Use
3. Simple and Intuitive Use
4. Perceptible Information
5. Tolerance for Error
6. Low Physical Effort
7. Size and Space for Approach and Use

The *Principles of Universal Design* were originally designed for the built environment and physical product design (Thompson et al. 2002). However this same philosophy can and has been implemented on a broader scale including education, user interface design and services (O'Leary & Gordon 2009). A product or service that incorporates these, arguably aspirational, principles is accessible and usable by everyone, irrespective of a person's background, skills or abilities (NDA 2012). For people with visual, physical or learning disabilities, universally designed technologies can remove barriers and obstacles that they would typically face day to day (Norman 2004). These universal designed products and services are simple and intuitive to use, flexible towards user's preferences, require minimum physical effort to use and have a high tolerance for error.

The *Principles of Universal Design* should be considered as a philosophy for good design rather than a strict list of principles that need to be implemented in their entirety. Many of the concepts within these principles overlap each other, and in some cases can contradict each other. For example, the principle of *Flexibility in Use* encourages designers to accommodate for a wide range of user preferences. While the merit of this principle is clear, providing users with a large number of preference settings can complicate a product and thus contradict the principle of *Simple and Intuitive Use*. Overall a balance needs to be found when implementing these principles to ensure good design.

An example of a universal designed product in the built environment is illustrated in Figure 12. The stairs meet the needs of a large number of users, with all the accommodations achieved in the one aesthetically pleasing design without stigmatization. Walkers can traverse the stairs one step at a time, wheelchair users can

navigate their way to the next floor using the ramps provided and elderly users can take advantage of the grab rails to ensure their safety.
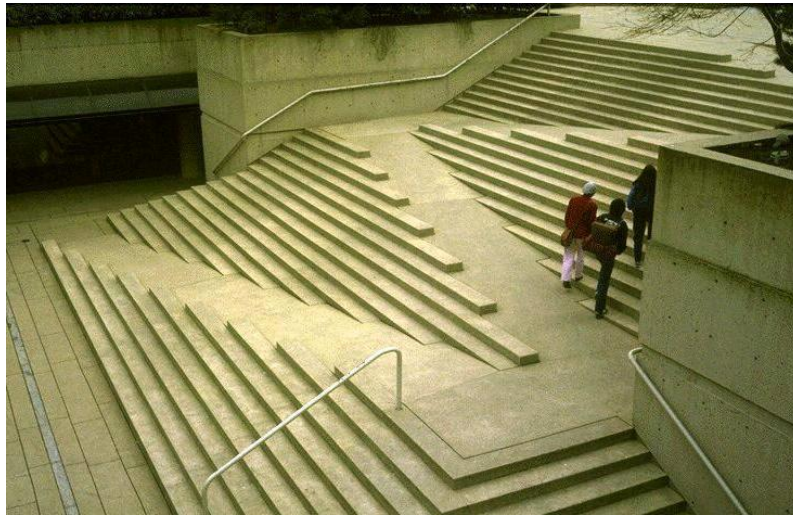


**Figure 12: Universal Designed Stairs (GreatBuildings 2012)**

In the domain of information technology, the Apple iPad is an example of a product that is universal designed, as illustrated in Figure 13. The iPad provides users with an inbuilt screen reader (VoiceOver) and switch access alternative (AssistiveTouch). This means that users with visual and physical disabilities can use this product without the need to purchase any extra assistive technology software or hardware. The Apple iPad uses simple language, instructions and menu systems ensuring people with varying computer and language skills can use the tablet with ease.



**Figure 13: Universal Designed iPad (Apple Inc. 2012)**

To ensure all applications developed on the iPad are universally designed, Apple encourages developers to follow their *User Experience Guidelines.*

## 2.6.2   Apple User Experience Guidelines

Apple's User Experience Guidelines outline how a developer can design an application to be easy and intuitive to use for all users.  These guidelines illustrate how a user interface should be visually designed and how it should behave to ensure the application is simple and intuitive to use. By developers adhering to these guidelines, new applications designed for Apple Mac products remain consistent with other iPad applications on the market.

These guidelines provide a developer with an understanding of how a user interacts with Apple applications from where the user looks on the screen to how they activate the application's controls (Apple 2010). The guidelines state that important user interface controls and information should be made obvious to the user using simple techniques like using a translucent toolbar on photo applications or fading controls after a user has stopped interacting with them (Apple Inc. 2010).

It suggests that the top of the screen is the most visible to users as they tend to hold the Apple device with one hand and operate it with the other. For this reason any important instructions or frequently used controls, like the back button, should be placed at the top of each screen.

In terms of textual content the guidelines encourage developers to use labels, titles and instructions that are clear and concise. Users should be able to read and understand all the information on an application's user interface quickly without any problems. To help with this user interface controls should use well understood symbols to further assist a users understanding of a screen (Apple 2010).

## 2.6.3   Web Content Accessibility Guidelines

The Web Content Accessibility Guidelines are designed to help developers create and evaluate accessible web content.

The first of these guidelines, *Web Content Accessibility Guidelines 1.0* (WCAG 1.0), were published by the Web Accessibility Initiative (WAI) in 1999 (WAI 2011). These guidelines directed web developers to provide accessible content that would operate correctly using assistive technologies and user agents (e.g. a web browser) that were available to Internet users at the time. However, with the advances in assistive technologies, browser enhancements and new programming language capabilities these guidelines became out dated (Reid & Snow-Weaver 2008).

To resolve this, a second version of these guidelines (*WCAG 2.0*) was published in 2008 (WAI 2011). *WCAG 2.0* consists of 12 guidelines that are categorised under four principles: perceivable, operable, understandable and robust. These four principles reference the same philosophy as outlined in the *Principles of Universal Design*. The guidelines have three priority levels A, AA and AAA, with A being the minimum. These guidelines are considered the industry standard for creating and evaluating accessible web content (WAI 2012). *WCAG 2.0* encourages developers to explorer new technologies and techniques in order to provide web users with informative alternative content were necessary (Sullivan & Matson 2000).

For screen reader users, it is important to provide alternative text on a web page. This means that any information conveyed by images, multimedia content or charts is still accessible to these users. The guidelines also stress the importance of device independence. Device independence refers to the ability to navigate through and interact with web content irrespective on the input device being used by the Internet user. Device Independence ensures that keyboard users, mouse users or switch access device users can interact with a website and its content with ease. Users with learning disabilities are also considered by *WCAG 2.0*. Web developer are guided to use simple language, provide alternative text for abbreviations and acronyms and encouraged to try to avoid displaying text section swith a width greater than 80 characters. This ensures that user with dyslexia can find it easier to read the information presented.

## 2.7 Accessibility Tools

### 2.7.1 International Classification of Functioning

Modern medicine relies on the sound measurement of health. Health can be described in a number of different ways, ranging from physical attribute like the body functions and structures to environmental aspects like how a person's participates in a given environment (Cieza et al. 2002).

The International Classification of Functioning (ICF) is a classification system that describes how people live with their disabilities and/or health conditions (CAD 2001). It is often used in clinical settings, health services or surveys to gain an understanding of health issues at an individual or population level.

The ICF system can assist with the assessment of patients' problems and outcome evaluations (Cieza et al. 2002). It classifies health and health related domains that describe the body's structures and functions while considering a person's activities and participation. A person's activity is described as the execution of a task or action. Participation is described as the involvement an individual has in a life situation (Perenboom & Chorus 2003). As activity and participation occur in the context of an environment, the ICF considers a list of environmental factors.

The ICF considers the concepts of health and disability in a different way from other classification systems (World Health Organization 2001). It takes into account that every person can experience health issues and therefore experience some level of disability, whether temporary or permanent. The ICF focuses on the impact of health conditions in the context of an individual's environment, rather than in the context of the medical and biological dysfunction (World Health Organization 2001).

### 2.7.2 Exclusion Calculator

The Exclusion Calculator, designed by the Engineering Design Centre at the University of Cambridge, is a design tool that is used to estimate the number of people that are excluded from using a product, illustrated in Figure 14. Designers can improve the accessibility of their products by understanding the number of people and the type

of disabilities that are excluded from product use. By meeting the needs of those excluded enables Inclusive Design.



**Figure 14: Exclusion Calculator**

Inclusive Design works on the same philosophy as Universal Design. It is defined by the British Standards Institute as,

> "*The design of **mainstream** products and/or services that are **accessible** to, and **usable** by, **as many people** as reasonably possible … without the need for special adaptation or specialised design"* (Coleman et al. 2011).

Inclusive Design places responsibility on designers, developers and those who commission production within the industry to produce accessible products (Coleman et al. 2007).

The Exclusion Calculator assesses a product's accessibility using the following categories (University of Cambridge 2009):

- **Vision**: This category measures the scale to which a person can use colour and light to detect objects, distinguish between different surfaces or identify details on a surface.
- **Hearing**: This category measures the scale to which an individual can distinguish speech from ambient noise or determine the direction in which the sound is coming from.
- **Thinking**: This category measures the varying capabilities an individual has with regards to processing information, processing memories and selecting appropriate responses and actions in a given context.
- **Communication**: This category measures how well an individual can understand other people and express themselves to other people.
- **Locomotion**: This category measures the movement capabilities an individual has, like moving around, bending down, sitting and standing.
- **Reach and Stretch**: This category measures how well a person can hold their arms in front of their body, above their head or behind their back.
- **Dexterity**: This last category measures the capability that an individual has to perform fine finger manipulation. This includes picking up and squeezing objects.

These categories and the metrics that they present used by the Exclusion Calculator are derived from a Family Resources Survey that was commissioned and conducted by the UK Government in 1997. The aim of the survey was to assist with planning welfare support for people with disabilities in the UK. Using these categories, 17.8% of the British population was identified as having a disability of some kind (University of Cambridge 2009).

## 2.8 Accessibility and Usability Testing

Usability is determined by how well a specific user group can complete a task, whereas accessibility is determined by how well a diverse group of users can complete a task. This correlates to Lang's suggestion that usability testing significantly aligns and

overlaps with accessibility testing (Lang 2003). The only difference in the two testing methods is that accessibility methods call upon usability testing using a  more diverse user group (W3C 2010).

## 2.8.1   Nielsen's Usability Measurements

Nielsen's usability measurements are designed to evaluate how usable a product is (Judy 2005). These measurements can be used as a design tool or as a testing tool (Nielsen 2003). Using these measurements during design can help designers and developers to better understand the positive and negative impact that their designs produce (Van Welie et al. 1999). Evaluating products using these measurements is a good method for obtaining data regarding a product's usage. It can determine errors in the system, latency issues and give an understanding to the overall user experience (Van Welie et al. 1999).

There are five characters that are assessed during this testing process; learnability, efficiency, memorability, failure rate and satisfaction (Nielsen 2003).

Learnability is described by how easy it is for a user to complete basic tasks during their first encounter with a product. Efficiency is described by how fast a user can complete a task once they have become familiar with the product. Memorability relates to how easily a user can re-establish proficiency following a period of time of not using the product. The failure rate characteristic refers to how many errors occur while an individual is using a product and how easy is it for that person to recover from these errors. The last characteristic is satisfaction which relates to the level of user satisfaction experience while using the product.

## 2.8.2   SUMI Questionnaire

The Software Usability Measurement Inventory (SUMI), published in 1993, is a method of measuring the quality of software from the user's perspective (Kirakowski et al. 1998). It assists with evaluating user satisfaction and detecting usability issues during and after the product design phase (ISO 2010).

The SUMI questionnaire is available in paper form and online allowing tester's to complete the questionnaire conveniently. The questionnaire consists of 50 statements to which a user can respond stating that they *agree*, *don't know* or *disagree*. Examples to some of these statements are as follows:

- *"The way that the system information is presented is clear and understandable"*.
- *"I would recommend this software to a friend"*.
- *"This software responds too slowly to inputs"*.
- *"I enjoy my sessions with this software"*.

The SUMI questionnaire is the *defacto* industry standard for collecting and evaluating user responses to software products (Kirakowski 2012).

## *2.9    Accessibility Motivations*

There are many laws and regulations in place around the world that are designed to support accessibility (Breaux et al. 2008). Products and services that comply with these laws and regulations will have a directly positive effect on people with disabilities.

### 2.9.1   United States of America

There are two key laws in place in the United States that protect the rights of people with disabilities; Section 508 of the Rehabilitation Act and Section 225 of the Telecommunications Act.

The Workforce Investment Act amended Section 508 of the Rehabilitation Act of 1986 by extending and strengthening technology access requirements. This act was passed in 1998 (McLawhorn 2001). Section 508 requires government and federal agencies to ensure that all electronic information technology that they use is accessible to government employees who have disabilities and to members of the public with disabilities who may need to use that technology (Poynter 2002). Electronic information technology includes any federal websites, intranet and computer software. Any state in the country that receives funding from the government under the Assistive Technology Act of 1998 must also adhere with Section 508. Many elements in Section

508 mirror that of the checkpoints listed in WCAG 1.0 (Kelly et al. 2005). With WCAG 1.0 now outdated by WCAG 2.0, Section 508 also needs to be updated. In 2006, the US Access Board began this updating process. The refreshed Section 508 standards are expected to be published in early 2013 (SSB BART Group 2011).

Section 225 of the Telecommunications Act of 1996 requires manufacturers to ensure all telecommunications equipment or software is made accessible if it is readily achievable. This means that if a product can be made accessible with little difficulty or expense, the manufacturer must ensure that this work is carried out. If the product is not readily achievable the manufacturer must ensure that their products are compatible with assistive technologies (Jaeger 2002, p.508).

### 2.9.2 Ireland

The Irish Disability Act 2005 requires that public bodies must only purchase goods and services that are accessible to people with disabilities. It also requires that electronic information technology being used by a public body must be accessible to people with visual impairments.

The Equality Act 2004 requires that public services, whether provided by the public sector or private sector, should be accessible to people with disabilities. Any infringement of this requirement is regarded as discrimination. This act encourages service providers to make communication technologies and web content accessible.

### 2.9.3 United Kingdom

In 1995 the UK government introduced the Disability Discrimination Act. This law makes it illegal to refuse service to a person with disabilities or provide people with disabilities a lower standard of service. This directive includes services that are provided through information technology. Service providers are required to ensure their websites, whether in the public sector or private sector, are accessible to people with disabilities. This act does not specify a standard in which these websites must adhere to, but government policies require websites to adhere to WCAG 1.0 Level AA.

In 2000, the Disability Rights Commission was appointed in order to enforce the Disability Discrimination Act. This commission had the powers to investigate and bring charge against nonconforming organisations.

## *2.10 Conclusion*

The definition of disability can be broken into the medical model and the social model. The medical model suggests that a person's disability is caused by a functional or structural body limitation. The social model suggests that it is social and environmental barriers that cause a disability. The social model believes that these barriers can be removed by making the built environment and technological environment accessible.

In the domain of information technology there are many guidelines, principles and legal motivations, like *Universal Design* and the *Web Content Accessibility Guidelines 2.0,* that encourage software designers and developers to implement software that can be used by all, including people with disabilities.

Information technology products can be tested for usability and accessibility using the philosophy of "usable accessibility". Usable accessibility incorporates usability measurements of efficiency, learnability, memorability, tolerance for error and user satisfaction into the inclusive nature of accessibility testing, ensuring that a product is usable and accessible to as wide a range of individuals as possible.

# 3 CAPTCHA

## 3.1 Introduction

CAPTCHA systems are used more than 200 million times every single day (Google 2012). CAPTCHA is an automated test that is designed to tell humans and computers apart, an example of which is illustrated in Figure 15.



**Figure 15: reCAPTCHA (Google 2012)**

Their aim is to produce a test that is easy for humans to solve but difficult for computers. This chapter explores this concept by examining the different CAPTCHA interfaces that are commonly used on the Internet today; text based CAPTCHA, audio based CAPTCHA and image based CAPTCHAs. For each of these CAPTCHA variations this chapter provides an understanding of the usability, accessibility and security issues associated with these tests.

## 3.2 CAPTCHA Definition

A CAPTCHA is a type of Automated Turing Test. It stands for "**C**ompletely **A**utomated **P**ublic Turing Test to **T**ell **C**omputers and **H**umans **A**part" (L. von Ahn et al. 2002). It was developed by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford in 2000. The CAPTCHA process allows a computer system to judge if a response given has been generated by a human being or by a computer system.

The aim of a CAPTCHA is to prevent automated systems (bots) from gaining access to account services on the Internet using a test that humans can pass easily but that bots cannot (L.V. Ahn et al. 2003).

## 3.3  Turing Test

CAPTCHA systems are often described as a reverse Turing Test. A Turing Test is designed so that humans can determine if a series of responses has been generated by a human being or a computer system. This concept was originally discussed by Alan Turing in his 1950 paper *Computing Machinery and Intelligence* (Turing 1950). In this paper Turing suggested that the question "Can Computers Think?" could be answered using a Turing Test. The purpose of a Turing Test is to correctly and accurately distinguish a human being from a computer system.

The process of the Turing Test was described in what Turing called the Imitation Game (Turing 1950). In this game a human judge asks a variety of questions to two mystery entities. One of these entities is a human and the other is a computer. Both entities respond to the questions asked and actively try to convince the judge that they are a human being. After analysing the answers, the human judge must determine which entity is the computer and which is the human. If the computer successfully fools the judge into thinking that it is a human, the computer passes the Turing Test. Since this paper, Turing's concepts and ideas have been widely debated. While some defend his paper and consider his ideas to be the birth of artificial intelligence, others attack his idea as being useless, harmful and inaccessible (Pinar Saygin et al. 2000).

In computer science today, the concept of the Turing Tests is still practised and has since been automated using the CAPTCHA system. There are many different types of CAPTCHA tests currently available to Internet users; text-based CAPTCHAs, audio based CAPTCHAs and image based CAPTCHAs.

## 3.4  Text-based CAPTCHA

A text-based CAPTCHA poses a user with a randomly generated test. A user is shown a sequence of distorted images, numbers or shapes and is then asked to type in that sequence of characters into a text field, as illustrated in Figure 16. The characters are often distorted using colours, lines and image warping. The CAPTCHA test is designed so that humans can easily read the text but that computer systems, like bots, cannot.

**Figure 16: Text-based CAPTCHAs (Duffy 2011)**

A text based CAPTCHA can resist attacks from bots based on the complexity of their text distortions, length of the words used and randomness (Adeyinka 2008). This resistance to attacks can be measured using three factors; Characters, Noise and Speed (Chandavale & Sapkal 2011). The strength in characters is measured by how large the character or word datasets are. The larger the datasets, the less vulnerable the CAPTCHA test is to brute force attacks. The strength in noise is measured by the success rate of an OCR when attempting to recognise the distorted words. The strength in speed is measured by how long it takes an OCR system to successfully pass a CAPTCHA test and how much computational power it requires (Chandavale & Sapkal 2011).

### 3.4.1 GIMPY

Gimpy was one of the first text-based CAPTCHA systems used on the Internet. It was developed by von Ahn, L. et al in collaboration with Yahoo to prevent bots and spammers from entering their chat rooms and posting unsolicited advertisements. GIMPY also protected Yahoo's email server from bots creating random free email addresses (Yan & El Ahmad 2008).

Gimpy selects predefined dictionary words and distorts the word. The predefined dictionary words are selected from a dataset of 600 words that are readily available on the Internet (Mori & Malik 2003b). The assumption here is that humans will still be able to read the text and therefore pass the test, but Optical Character Recognition (OCR) systems will not. In order for a human to pass this type of CAPTCHA, the user

must identify three words out of the seven to ten words displayed (Mori & Malik 2003b). An example of a Gimpy CAPTCHA is illustrated in Figure 17. With the use of dictionary words and the relatively simple text distortions, it is possible for OCR technologies to solve the Gimpy test (Yan & El Ahmad 2008). The OCR works under the assumption that the colour of the text in the test will always have the lowest intensity of colour used. The OCR identifies this colour, removes all other colours from the test that do not match this text colour and therefore can easily extract the character sequence and solve the test. OCR systems are able to solve the GIMPY CAPTCHA with a success rate of 33% (Mori & Malik 2003b).



**Figure 17: Gimpy CAPTCHA Test (Mori & Malik 2003a)**

Another GIMPY solution called EZ-GIMPY also uses background noise to distort the character sequences. A way in which background noise can be implemented is to use a background colour that is of the same shade range as the text colour. This type of EZ-GIMPY was most commonly used by Yahoo (Mori & Malik 2003b).



**Figure 18: EZ-GIMPY CAPTCHA Test (Mori & Malik 2003a)**

EZ-GIMPY can be easily solved by automated systems using the same principles that are used to solve the original GIMPY test. OCR systems can successfully pass the EZ-GIMPY CAPTCHA at a rate of 92% (Thayananthan et al. 2003).

GIMPY-r is another variant of EZ-GIMPY. The GIMPY-r system differs from EZ-GIMPY by using non-dictionary words consisting of 4 characters. These characters are warped and distorted in a similar fashion to that of the first GIMPY implementations. Further distortions are added by using different fonts and complex background colours and patterns to create background noise, like boxes, grids, waves and ripples (Moy et al. 2004), as illustrated in Figure 19. However, this background noise often makes it difficult for visual users to recognize the character sequences and therefore makes it difficult for them to solve the GIMPY-r (Yan & El Ahmad 2008).



**Figure 19: GIMPY-r CAPTCHA Test (Mori & Malik 2003a)**

OCR systems can solve the GIMPY-r tests with a success rate of 78% (Moy et al. 2004). This indicates that the OCR systems have become increasingly advanced and can solve the Gimpy CAPTCHA tests whether the text is distorted by warping or background noise. This has lead to the text-based CAPTCHA systems distorting characters using character segmentation puzzles.

### 3.4.2 Google CAPTCHA

The original Google CAPTCHA system is a good example of a CAPTCHA test that distorts its character sequences using character segmentation distortions. It does this by removing whitespace from in between each character. This process makes it difficult for bots to segment each character, which in turn means that the bot cannot correctly identify each character used and therefore cannot solve the CAPTCHA test. With this, the segmentation distortion process of crowding characters together is currently considered the most advanced in terms of CAPTCHA security with an OCR success rate of only 12% (Yan & El Ahmad 2008). However, this segmentation process can cause serious issues as the characters can be hard to identify even for sighted users (Yan & El Ahmad 2008).
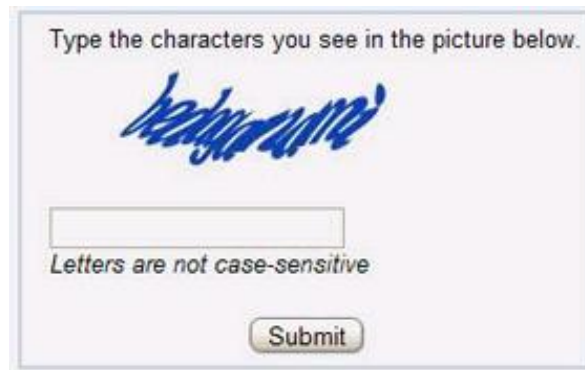
**Figure 20: Google uses text crowding techniques to distort words**

In 2009, Google acquired reCAPTCHA (Luis Von Ahn & Cathcart 2009). Following this, Google replaced their original CAPTCHA with the reCAPTCHA system.

### 3.4.3  reCAPTCHA

reCAPTCHA is a little different than a normal CAPTCHA test. Its main objective is still to determine if the user is a human or a computer, but it also has a second purpose that involves group participation. In the attempts to digitally scan and archive physical books that were written before the age of computing, multiple projects around the world are scanning in the pages from millions of books and using Optical Character Recognition to convert this information into a digitalised text format. However due to poor quality printing press issues some of the words that are scanned in cannot be correctly identified by the OCR systems (L. Von Ahn 2009). To resolve this issue reCAPTCHA presents the user with two character sequences. One of the character sequences used is the word that the OCR system could previously not identify (the unknown word); the other character sequence is the real CAPTCHA test (the control word). With each reCAPTCHA test, many users around the world are presented with the unknown word. Over time when enough users submit the same identical answers for the unknown word, the reCAPTCHA system is able to determine the true identity of this word. Following this the identified word is then added into the digitalised book from which it came from (L. Von Ahn et al. 2008). To explain in detail:

1. An OCR system encounters the following image of text and is unable to determine what it is:
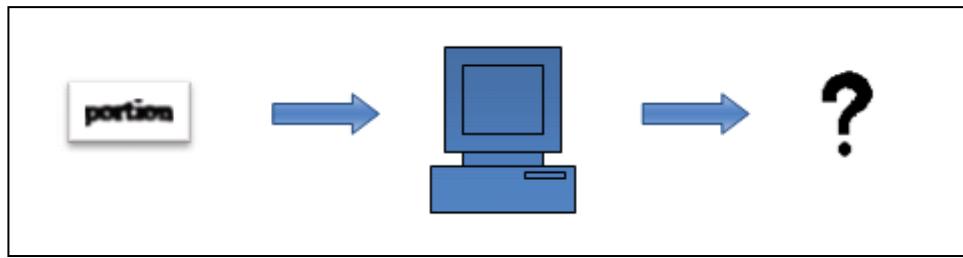
**Figure 21: reCAPTCHA unidentified word**

2. The unknown piece of text is used in reCAPTCHA which allows humans to identify the text:
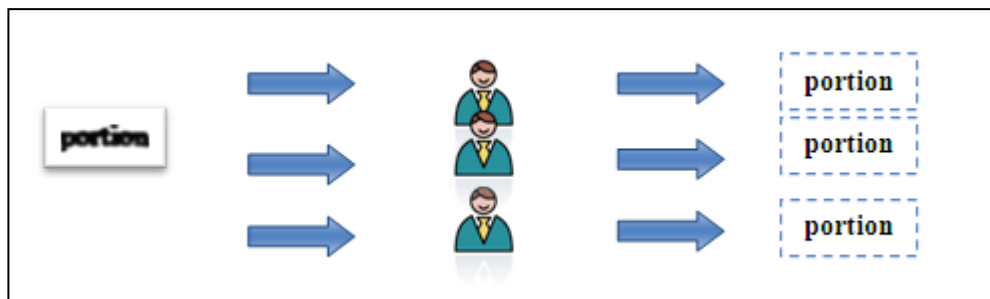


**Figure 22: reCAPTCHA User Input**

3. When enough of the same answers are returned from the user, the system builds confidence that the word has been correctly identified and it is this newly identified word that is added to the digitized book.
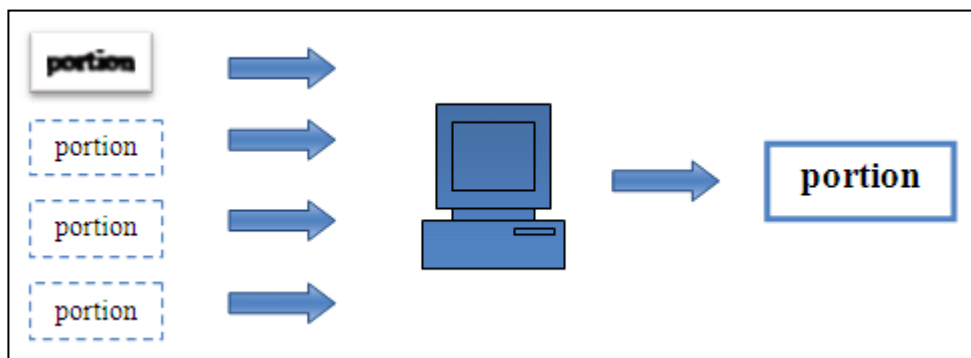


**Figure 23: reCAPTCHA word identified**

The human success rate for the text based reCAPTCHA is 90% (L. Von Ahn et al. 2008). reCAPTCHA also provides users with an audio CAPTCHA option in the case that the text based system is not accessible to them.

## 3.5 Audio CAPTCHA

Text based CAPTCHAs are unsolvable by people who have visual impairments. For this reason, soon after the release of the text based CAPTCHA, audio CAPTCHAs were introduced as an accessible alternative for the blind and visually impaired (Bigham & Cavender 2009). Although the adoption of this alternative was slower than that of the text based CAPTCHA, most popular sites like Facebook, Google, Yahoo, Microsoft and PayPal now include the audio CAPTCHA as an alternative. In order to resolve an audio CAPTCHA test, a user must first listen to an audio representation of a sequence of characters. The user can then type the characters heard into the input field provided. At first glance it seems that this type of CAPTCHA is similar to the text based CAPTCHA, with the only difference being that of the cognitive process required. Instead of using a human's visual perception, the human's audio perception is required to solve the test. However there is quite a difference with how a user interacts with each form of CAPTCHA test. This difference can cause major difficulties when solving the test for those who are blind and visually impaired (Sauer et al. 2008).

The CAPTCHA interface was originally designed to be a text based test, but following accessibility concerns, an audio version of the test was simply added on to the pre-existing CAPTCHA interface (Sauer et al. 2008). This has meant that users with visual impairments are required to interact with the system a little differently than visual users. When a sighted user interacts with the CAPTCHA interface, they can type their answer into the input field provided while also continuing to examine the characters in the sequence. This makes solving the test a little easily as users can take their time examining the CAPTCHA test one character at a time. However, audio users cannot interact with the test in this way. The audio playback cannot be paused at any point which means that the user cannot attempt to solve this test one character at a time. Instead, audio users must first listen to the linear playback, navigate to the input field,

give it focus and type in the answers as they hear them. User must type in every word they hear. Any missing words or spelling mistakes deems the test attempt a failure.

Another issue faced by the audio CAPTCHA is trying to find the correct balance between the usability of the interface so that humans can still solve the test while maintaining a level of complexity so that automated agents cannot solve the test. Traditionally most of the bot attacks were focused on the text based CAPTCHAs. However, recently audio CAPTCHAs have become a target (Bigham & Cavender 2009). With this, the quality of the audio playback in the audio CAPTCHA test has been modified in the attempts to ensure bots with speech recognition capabilities cannot solve these tests. The playback is distorted using background noises, such as unidentifiable chatter or music. This can make the words said in the audio test harder to identify by humans. This issue in itself is exaggerated even further if the user is using a screen reader. The screen reader is designed to present the content on a web page in an audio format for blind and visually impaired users. The screen reader can often talk over the audio CAPTCHA test, making the test even more difficult to solve. With these difficulties the audio CAPTCHA has been shown to have a very low success rate of only 43% (Bigham & Cavender 2009).

reCAPTCHA recently revised their audio CAPTCHA tests due to security vulnerabilities that were found with the system. This new implementation was released recently in May 2012 (Goodin 2012). To allow us to quantify how this new implementation has affected human usability, testing with the reCAPTCHA audio test was conducted as part of this project. It was found that this newer version of the audio reCAPTCHA test had a very low success rate of only 4%. More information regarding these test results can be found in Section 7.3.

## 3.6  Image Based CAPTCHA

An image based CAPTCHA offers an alternative to the common text-based CAPTCHA, by requiring a user to perform image recognition tests instead of text or audio recognition tests (Elson et al. 2007). Users are presented with one or more images and are asked to identify the object in the picture. Similar to the other CAPTCHAs discussed, image based CAPTCHAs are designed so that humans can

easily identify the objects in the displayed images and therefore pass the test, but bots cannot. However, there are security issues associated with image based CAPTCHAs.

Firstly all images used in an image based CAPTCHA tests are pulled from a centralised database. Each image entry is mapped to a textual label. On average, image-based CAPTCHAs usually present a user with 4 − 8 images at a time. This means that an automated system can potentially solve the CAPTCHA test using brute force (Elson et al. 2007).

Secondly the strength of an image-based CAPTCHA relies heavily on the size of its database. If the database is too small the same images will begin to repeat themselves in each test and therefore an automated system can begin to build its own database of the images and their labels used and eventually solve the test easily. Large databases mean that images are less likely to be repeated often and therefore automated agents cannot build a copy of the database easily (Elson et al. 2007). However even with a large database, once the database is compromised the entire CAPTCHA system is rendered useless. Text-based systems do not have this problem as the character sequences are not stored in a database. Instead the letters and words are generated and distorted randomly at runtime.

### 3.6.1   PIX CAPTCHA

The PIX CAPTCHA was the first implementation of an image based CAPTCHA. The PIX CAPTCHA uses a database that is manually populated with images and their associated labels. As this database is manually populated the database size remains relatively small. This leads to easy duplication of the database by attacking bots, which meaning that the bots can easily solve the CAPTCHA tests. To resolve this issue, the database needs to be larger using an automated process.

One of the first automated database generation processing was first introduced in 2004 by Chew and Tygar (Elson et al. 2007). They used an automated system to generate a database of images and labels from image search results retrieved from Google's search engine. This database generation, however, was not successful. Google categorises images based on the text that surrounds the image. This text, although may

be relating to the image, may not accurately classify the image. For example, the word honey may refer to an image of a pot of honey, a bee hive or even a person's loved one. Another flaw in this database technique is that if the creator of the CAPTCHA test can generate a database of images using an automated approach, a hacker can create a similar automated process and in theory generate the same database of images with the same mapping of labels.

## 3.6.2   ESP PIX CAPTCHA

A solution to this database generation problem was described by von Ahn et al (L. Von Ahn & Dabbish 2004). He devised a system that would ask human beings to label and classify images themselves. This task was masked as a game called the "ESP Game" (L. Von Ahn & Dabbish 2004). This game required two non-communicating players to label images that were presented to them on their computer screen. If the two players labelled the image with the same word they would get a point. All the images used and most frequently used label mappings were added to a separate database to be used later for the ESP PIX CAPTCHA test.



**Figure 24: ESP PIX CAPTCHA**

During the ESP PIX CAPTCHA test, a user is presented with 4 images and a menu with a selection of 70 possible labels that could be used to classify the image. From this collection there is only one possible answer, which is the label that has been used the most to describe the image by other users. It is this technique that makes the test a

potential target for brute force attacks. Even though the database can be very large, meaning that automated agents cannot duplicate it, bots can simply select a label item at random from the collection of 70 labels and eventually solve the test.

Overall humans can solve the ESP PIX CAPTCHA with a success rate of 85.44% (Vimina & Areekal 2009). The reason for failures can often be related to the fact that sometimes the labelling of image can be a little abstract and subjective. For example, a user may be presented with the image of a heart. The user selects the "heart" label and submits the test only for the test to fail. What the user did not realise is that the image was labelled as "love" and not as "heart".

### 3.6.3   Assira

A common image based CAPTCHA that attempts to resolve many of these usability and security concerns associated with image-based CAPTCHA is called Assira. This CAPTCHA test was introduced in 2007 (Elson et al. 2007). The test presents users with 12 images depicting either a cat or a dog. The user is then asked to identify and select the pictures that display a cat in them. Assira has a human success rate of 99.6%, with each test being solved in under 30 seconds (Golle 2008). It is calculated that an automated agent only has a 1/4,096 chance of solving the test using brute force (with the assumption that the database is never compromised) (Elson et al. 2007).



**Figure 25: Assira's Image-based CAPTCHA**

Assira's images are pulled from a large database that is controlled and populated by one of the largest animal adoption websites, Petfinder.com. This database has over three millions images of cats and dogs, with 10,000 new images added daily (Elson et al. 2007). The sheer size of this database makes it more secure as it would be difficult for a bot to duplicate it. However, the Assira CAPTCHA is still vulnerable to OCR attacks. It has been shown that automated systems can be used to identify the animal in each image with a success rate of 82.7% (Golle 2008).

## 3.7 CAPTCHA Metrics

It is difficult to determine the strength of a CAPTCHA test, as the cost of a human failure differs from the cost of a bot failure. A human may happily repeat a CAPTCHA test if they fail it once and therefore the cost of their initial failure is low. However, if the burden to pass a CAPTCHA test is too large for a human it may discourage them from using the online service, in which the cost of their failure is high. Chellaphilla et al takes this cost of failure into account in their paper "*Designing Human Friendly Human Interaction Proofs (HIPS)*" and determine that a strong CAPTCHA system should have a human success rate of 90% and a bot success rate of 1% (Chellapilla et al. 2005).

The previous section discussed the human success rates of the text based CAPTCHA, audio based CAPTCHA and image based CAPTCHA. A summary of these results are outlined in Table 2.

**Table 2: Summary of CAPTCHA Human Success Rate**

| CAPTCHA Type | Human Success Rate |
|---|---|
| Text Based reCAPTCHA | 90% |
| Audio CAPTCHA | 34% |
| Image Based Assira | 99.6% |
| Image Based ESP PIX CAPTCHA | 85.44% |

The results observed from the text based and image based CAPTCHAs would suggest that these type of CAPTCHA systems have a relatively high human success rate. However, the testing methodology used to retrieve these results is not discussed in any of the relevant research. The number of testers used in these experiments is not indicated, nor is the testers' profile outlined. This would suggest that these testing results are flawed. In order to establish a true human pass rate for these various CAPTCHAs, testing would need to be conducted using between 10-20 testers (Faulkner 2003). To achieve a true representation of the accessibility and usability of these CAPTCHA systems, these testers would need to exhibit a broad range of characteristics, including age, skills, language and disabilities (W3C 2010).

Text based CAPTCHAs have many accessibility and usability issues associated with them. Blind or visually impaired users are unable to see the image of the distorted text so therefore cannot pass a text based CAPTCHA. Users with learning difficulties, like dyslexia, may also find it difficult to correctly identify the characters in a text based CAPTCHA and therefore fail the tests. In the experiment outlined in Section 6, this theory is explored.
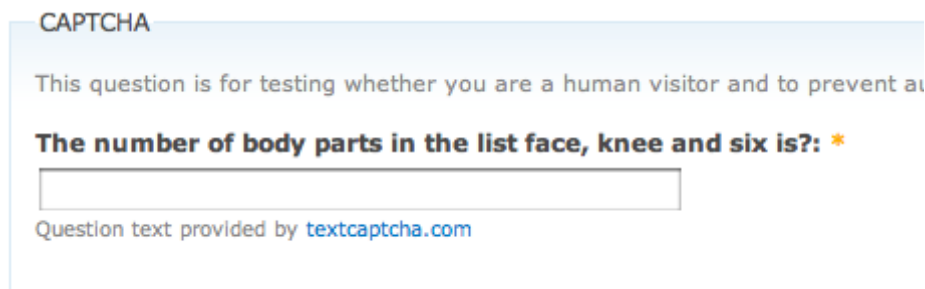
Image based CAPTCHAs remove many of the usability and accessibility concerns for users with learning difficulties, however, users with visual impairments still face the same challenges as they do with text-based CAPTCHAs. As this test is purely image based, users who are visually impaired or blind cannot solve them and must resort to using the audio based alternative test in order to progress forward in the site.

In Bigham and Cavender's paper "*Evaluating Existing Audio CAPTCHAs and an Interface Optimized for Non-Visual Use*", a methodology was outlined for testing audio CAPTCHAs. Testing was conducted with 89 blind testers (Bigham & Cavender 2009). The audio CAPTCHA is designed to be the accessible alternative to text based and image based CAPTCHA tests, however, with a success rate of only 43%, this indicates that this alternative is a weak CAPTCHA system (Chellapilla et al. 2005) and is inaccessible for many users.

## 3.8 Alternatives to CAPTCHA

### 3.8.1 Logic puzzles

A logic CAPTCHA test is a test that asks a human a question that requires simple knowledge to answer (Tuley 2011). For example a logic capture CAPTCHA may ask what day in the week comes after Wednesday or what type of animal barks. This type of test is illustrated in Figure 26.



**Figure 26: Logic CAPTCHA puzzles (Tuley 2011)**

### 3.8.2 Semantic CAPTCHA

A semantic CAPTCHA is a CAPTCHA test that requires a human to make sense of a given sentence. Users must use some type of semantic reasoning in order to pass the test (C. J. Hernandez-Castro et al. 2010). A semantic CAPTCHA test may involve a user completing a sentence with a missing word, for example "Stopwatches can _____ numbers". One limitation of this type of test is that the answer may sometimes be subjective. The answer to the above question could be "count", "time", "display" or "show".

### 3.8.3 Single Sign-on

A single sign-on system allows a user to gain access to multiple online resources using a single authorisation system (Groß 2003). This means that an individual registers with an identity provider, and this identity provider then provides global or local authentication to other parties or service providers (Pfitzmann & Waidner 2003).
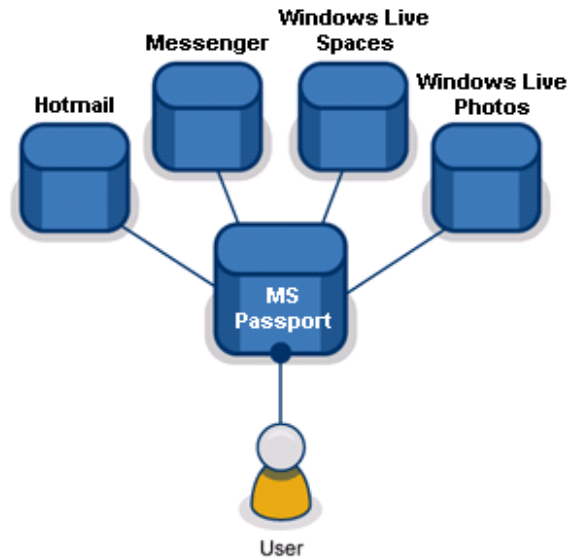
**Figure 27: Microsoft Passport Network (Atlassian 2012)**

An example of a single sign-on system is that of the Microsoft Passport system, as illustrated in Figure 27. A user can create an account with Microsoft by providing their details, a username and a password (Dongwan Shin et al. 2004). Once a user signs into this account they can access many of Microsoft's online resources without the need to sign in again. This means that users can access Microsoft's email, messaging services and social networking systems using one log in facility.

Single sign on systems aims to provide a secure and convenient authorisation system. The intention is that an electronic identity is only given to the person that it belongs to meaning that the user's identification cannot be attacked or used incorrectly.

### 3.8.4 Biometrics

The World Wide Web Consortium (W3C) suggest that an alternative to traditional CAPTCHA is to use biometric data to identify if a person is a human or not. They explain that this biometric solution could be implemented in conjunction with a single sign-on logon account (W3C). This type of system would capture the relevant biometric data of a human being and then use this data to create a unique user account for the individual.

## 3.9   Conclusion

There are many variations of CAPTCHA available to Internet users; text based CAPTCHA, audio based CATCHA and image based CAPTCHA. In order for these types of CAPTCHA tests to be successful, they must have a human success rate of 90% and a bot success rate of 1%. Previous user testing conducted using some of the text based and image based CAPTCHA tests suggests that these type of systems exhibit a human success rate of over 90% or lower. However, the methodology used in these tests was not outlined in any of the research. This might indicate that a wide range of testers with varying skills and abilities were not used during this testing and therefore does not reflect a true human success rate result in terms of usability and accessibility. The audio CAPTCHA, designed to be the accessible alternative has a human success rate of 43% which also indicates a low accessibility and usability rating.

The World Wide Web Consortium (W3C) suggest that an accessible and usable alternative to text based, audio based and image based CAPTCHAs is in the use of human biometrics. In the next chapter this area of biometrics is explored.

# 4   BIOMETRICS

## 4.1   Introduction

This chapter examines the existing literature and research in the area of biometrics. It provides a definition of biometrics, discussing the origins of the name and the various characteristics associated with biometric technology. It outlines how a biometric system can be used for both identification and verification, while also explaining the differences in these types of authorisation systems. Following this, the chapter discusses the various types of physiological and behavioural biometric data that can be captured and examined by a biometric system, including fingerprint, retina, voice, and face recognition systems. A summary is provided regarding the current usage of biometrics systems and some of the security issues faced by these systems.

## 4.2   Definition of Biometrics

The term *biometric* originates from the two Greek words; *bios* meaning life and *metrikos* meaning measure (Prabhakar et al. 2003). In the field of information technology the term *biometric* is defined as *"any automatically **measurable**, **robust** and **distinctive** physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual"* (Woodward Jr et al. 2003).

**Measurable** biometrics means that an individual's traits or characteristics can be acquired using biometric sensors and converted into a quantifiable digital format. This digital format of biometric data is called a Biometric Template (A. K. Jain et al. 2008). There are ISO standards that document how these templates should be constructed. For example the ISO standard ISO/IEC 19794-2 outlines how fingerprint data should be represented in these data files (Standardization 2011).

People's biometric traits and characteristic are subject to change over time. These variances in biometric data can be caused by a person's age, health or occupation. The extent in which a person's biometrics can change is referred to as the **robustness** of biometrics. For example, a person's iris biometric data is considered to be highly robust because a person's iris does not change significantly over time (Lim et al.

2001). An example of a less robust biometric is a person's voice as it is subject to change with age, emotion and environment.

A biometrics **distinctiveness** relates to how unique the biometric data is compared to the general world populate. The more distinct the biometric data is, the easier it is to uniquely identify an individual. A person's retina biometric data has a higher level of distinctiveness (Delac & Grgic 2004) than an individual's hand geometry (A. Jain et al. 2002).

Biometric data that is measurable, robust and distinct can be used to identify or verify an individual during an authorisation process.

## 4.3  Identification and Verification

Identity recognition systems are used to uniquely identity human beings. It does this by acquiring information from a user, extracting out a feature set from this data and then comparing this information against other feature sets in a database. An individual's identity can be authorised based on knowledge, ownership and biometric data (Xiao & Defence 2002).

Knowledge authorisation works on the basis that a user knows some unique information that will help identify them, like their username and their personal identification number (PIN). A security system using knowledge authorisation assumes that the user can remember their username/ PIN combination and also that no one else has acquired these logon credentials.

Ownership authorisation works on the basis that the user is carrying something on their person that can uniquely indentify them, like a magnetic strip card or a key. A weakness with this type of authorization mode is that personal identification numbers and smart cards can be easily forgotten, lost or stolen.

Biometric authorisation means that users can be authenticated based of their unique physical or behavioural characteristics like their fingerprints, retina, voice and/or face

information using various different biometric sensors. This means that this type of identification data presented by the user cannot be forgotten or lost by the individual.

When establishing an individual's identity using knowledge, ownership and biometric data, authorisation systems can operate in two different modes depending on the context of the application; verification mode and identification mode (Prabhakar et al. 2003).

The verification mode is a more traditional authorisation process which is used to determine if a user is who they say they are. The system does this by retrieving two elements of data from the user and then comparing this information to see if it maps correctly using a one-to-one comparison (Hong & A. Jain 1998), illustrated in Figure 28.
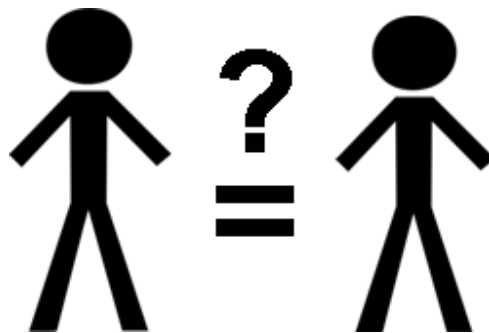


**Figure 28: Verification Mode One-to-One**

In this mode, a user claims their identity by presenting their username or smart card along with a password or personal identification number. If the two elements of identification data match, the system will determine a positive recognition. This mode is generally used to ensure multiple users do not gain access to the system by using the same identity (A.K. Jain et al. 2004).

The second mode of authorisation of an identity recognition system is the identification mode. This type of system is designed to acquire one element of identification and compare it to all the data entries contained in a database, as illustrate in Figure 29. Using this one-to-many comparison method, the system can find a match

in the database and therefore identify the user correctly (Daugman 2004). If a match is found the user is granted access to the restricted areas of the system.
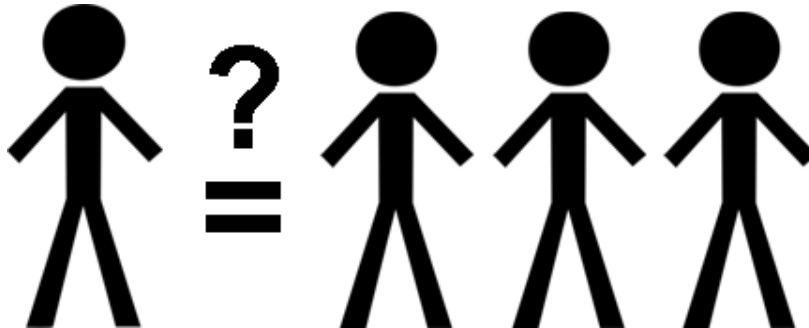


**Figure 29: Identification Mode One-to-Many**

This mode uses a negative recognition method meaning that the system determines who the user is not before it establishes who the user is. This type of recognition mode is generally used to ensure one user cannot have multiple identities. Negative recognition can only be successfully conducted using biometric information (Faundez-Zanuy 2006).

Biometric authorisation systems can capture an individual's physiological biometric data like their fingerprint or retina, or an individual's behavioural biometric data like their voice or handwriting.

## *4.4 Physiological Biometrics*

Physiological biometrics relates to biometric data that is collected by measuring parts of the human body. Fingerprint recognition and retina recognition both belong to this biometric group (Faundez-Zanuy 2005).

### 4.4.1 Fingerprint Recognition

A fingerprint consists of a series of ridges and furrows on the surface of a finger. These ridges and furrows produce distinctive patterns and minutiae points as illustrated in Figure 30. Minutiae points are local ridge characteristics that occur at either ridge

bifurcations (when a ridge divides into two) or ridge endings. It is these points that determine the fingerprint's uniqueness (Cheng & Larin 2007).
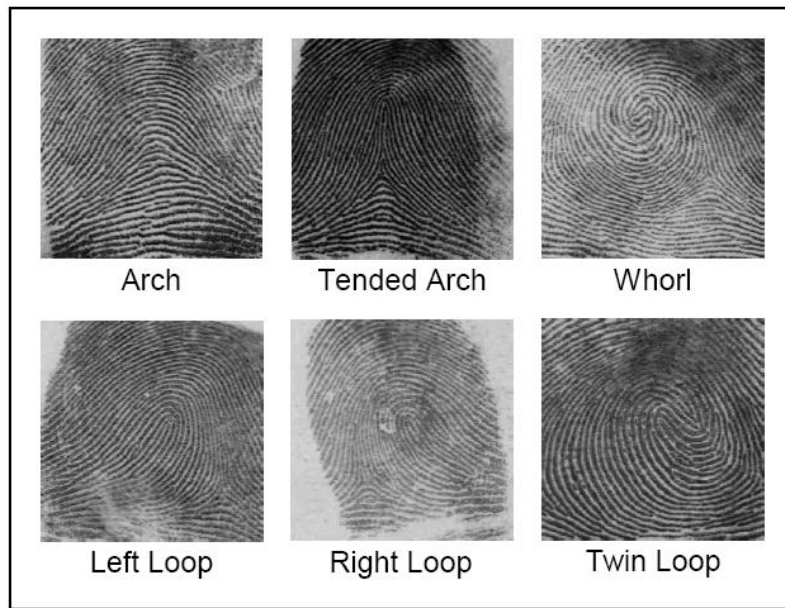


**Figure 30: Patterns of Fingerprints**

Fingerprint recognition has been used as a means to uniquely identify human beings since the 19th century (Cole 2004). Each finger on a human hand has a different fingerprint and each finger print is unique to an individual (Dugelay et al. 1993). Fingerprint recognition was first used by large law enforcement departments to identify criminals, a process that is still used today. The police departments began with collecting the fingerprints of all the criminals in their prisons and storing this information in a paper database (A. Jain et al. 2002). At a scene of a crime, the police department would attempt to retrieve any fingerprints left at the scene. Using these lifted prints, the police would consult the paper database to see if they could find a match for the prints and therefore identity the perpetrator (Cole 2004). Nowadays, fingerprint recognition systems are used across many different fields, and not just for criminal identification.

Fingerprint recognition sensors are readily available on the market, and are becoming more affordable for a large number of applications. The accuracy of fingerprint recognition is often determined by the computational power that the system has available to it (A.K. Jain et al. 2004). Large fingerprint recognition systems store

millions of user information and fingerprint mappings. When using an identification mode system, acquiring data from a user and then comparing this data to all the entries in the database can be very process intensive.

In terms of accessibility, fingerprint recognition is not always possible. Factors include aging, environment (temperature and humidity) or occupational reasons (for example a carpenter may have a variety of cuts on their fingerprints that keep changing day to day). Even without these factors finger print recognition may not always produce an exact match (Kang et al. 2003). Two fingerprint samples taken from the same finger of an individual will not always exactly match because of differences in the user's interaction with the system. For example, a user may place their finger on a fingerprint scanner differently each time a sample is taken. For this reason, the aim of fingerprint identification is not to find an exact match, but to score the fingerprint sample in terms of their similarities using the print's minutiae points. The higher the score, the more likely it is that a match has been found.

One of the major limitations for using fingerprint recognition is that even when a match is found, a correct identification cannot be assumed. This is due to the fact that fingerprints can easily be forged. These forged fingerprints can be constructed by making moulds of a person's fingerprint and casting them with gelatine, silicone or latex, as illustrated in Figure 31. These casts can then be used to fool a fingerprint scanner (Antonelli et al. 2006). A fingerprint reader can be fooled using this mechanism with a success rate of more than 67% (T. Matsumoto et al. 2002).



**Figure 31: Fingerprint Forgeries**

4.4.2   Retina Recognition

Retina biometric recognition involves capturing an image of the layer of blood vessels that are located in the back of the eye (Wildes 1997). The system captures this image

by streaming a low intensity light source through an optical coupler and scanning the patterns of the blood vessels in the retina, as illustrated in Figure 32. These patterns seen in the retina can change in a human's lifetime. These changes can be caused by diabetes, glaucoma (Gao and Hollyfield, 1992) and aging (Mizutani et al., 1998)



**Figure 32: Image captured by retina scanner**

A retina scanner requires that a user place their head next to the scanner, usually supporting their chin on a rest provided by the scanner, and focus on a defined point. In order to achieve an accurate reading, users must remove their glasses. Users can often feel uncomfortable when user a retina scanner as they are required to place their eye very close to the device (Guru et al. 2011). Because of this usability issue, retina scanning is often not warmly accepted by users (Liu and Silverman, 2001).

### 4.4.3   Facial Recognition

In the natural world, facial recognition is the most common way that human beings process a personal identification. The ability to recognise face and estimate people's expressions plays an important role in an individual's social life. Nearly 30 years ago, the first model of face recognition was presented by Bruce and Young (Bruce & A. Young 1986). This model posited independent neurological routes for the recognition of facial expression and facial identity. For example, the familiarity of a person's face does not affect how an individual reads the person's facial expressions (Haxby et al. 2000). Still to this day, this framework has remained the leading account of face perception (Calder & A. W. Young 2005). Today, facial recognition software can be used to recognise a person's facial expressions (a feature that is used in many digital camera software) and also to identity an individual's face.

In facial recognition software, an individual's face can be recognised both statically by using a photograph or dynamically using real time video capturing. These systems use a variety of data from a human's face including the location and dimensions of the eyebrows, eyes, nose and chin (Brunelli & Poggio 1993). The accuracy of facial recognition is still a point of weakness for these systems. It has been shown that static face recognition systems can easily be forged by holding a picture of a person up to a face scanner (Juels et al. 2005).

In theory, facial recognition software should be able to identify a human using any image irrespective of the background of the photo and the viewpoint in which the image is captured. In reality though mainstream facial recognition software have many limitations. Firstly, facial recognition systems often require a high level of image quality to ensure correct identification (Zhao et al. 2003) . This involves capturing the same facial orientation each time and ensuring that the lighting conditions are consistent. If a system captures a human face from a different angle or with poor quality lighting it can be difficult to produce a correct identification (Adini et al. 1997). However with the use of view-based formulation systems, individual's faces can be recognised under varying head orientations as long as the person's eyes, mouth and nose are captured in the image (Pentland et al. 1994).

An example of a facial recognition application is the SmartGate system used in Australia's international airports. The SmartGate system allows travellers that are arriving in the airport to process themselves through passport control. Eligible travellers do this by scanning their passport and face into a specially designed kiosk, as shown in Figure 33. Using these details the system can verify the traveller.



**Figure 33: Man using SmartGate system in airport (Australian Customs Service 2012)**

Once the traveller has been successfully identified by the system, background custom and immigration checks are conducted in an automated process. This SmartGate system enables travellers to bypass the traditional customs and border protection officers, saving the traveller time and the airport money (Australian Customs Service 2012).

## 4.5 Behavioural Biometrics

Behavioural biometrics relates to data and measurements acquired from an individual's actions. Voice recognition and signature recognition are examples of this biometric group. Processing this type of biometric data can often require some artificial intelligence as this type of data is subject to change (Faundez-Zanuy 2005). For example a person's voice can change day to day depending on the individual's current emotional state.

### 4.5.1 Voice Recognition

The human voice is characterised by physiological and behavioural factors. Physical characteristic such as the size and shape of an individual's vocal tracts, tongue and lips affect the pitch and frequency of the voice (Halle & Stevens 1962). Behavioural characteristic like age, medical conditions, emotional state and geographical location also add variance to the human voice. Voice recognition systems can be text-dependent or text-independent. Text-dependent systems have predefined phrases that users can say to identify themselves to a system. Text-independent systems allow users to identify themselves by saying any phrase they wish. These text-independent systems are more difficult to design as they must be more dynamic but they offer a more secure and fraud resistant voice recognition system when implemented correctly (Reynolds & Rose 1995).

In terms of voice recognition, it can be difficult to identify a person accurately and securely (A.K. Jain et al. 2004). Family member's voices can often sound very similar, plus humans can be trained to vocally mimic each other. The quality of the microphone which is capturing the human voice is another factor that needs to be considered. The microphone used must be able to remove background noise without distorting the recorded human voice.

A common implementation of voice recognition can be seen in speech recognition software. Speech recognition software is not used to uniquely identify an individual, but to synthesise a person's speech to text. These systems can either be speech-dependent or speech-independent (Huang & K. F. Lee 1993). A speech independent system is a system that must be trained to recognise an individual's voice. Although this system needs more time devoted to training it, it has a higher recognition accuracy rate. A speech independent system can be used without the need to train the system. This means a user can begin to use the system immediately but the accuracy of the recognition system is compromised.

In terms of applications of voice recognition, the Australian Health Management (AHM) organisation offers their members the option of identifying themselves to an automated telephone system by using their voice. Members say their name and membership number aloud. The system records this voice data and verifies that the individual is who they say they are (Alver 2007).

### 4.5.2 Handwriting Biometrics

Handwritten signatures are commonly used to authorise financial transactions and legal documents (Krawczyk & A. Jain 2005). Due to the high level of acceptance and wide spread usage of signature authorisation, a lot of research has been conducted in this area in the attempts to automate this authorisation process (Nelson et al. 1994).

In the area of information technology, handwriting biometrics is commonly collected using a sensor pad and stylus. A person's handwriting characteristics are examined by measuring the shape of each individual handwritten letter and by measuring the pressure and velocity in which the stylus moves across the sensor pad (Delac & Grgic 2004).

Similar to face recognition, there are two modes of signature recognition; static and dynamic (Sayeed et al. 2007). Static recognition (also called off-line recognition) involves an individual writing their signature on a piece of paper. The signature is then transformed into a digital template using an optical scanner or camera. Biometric

recognition software then analyses this signature in terms of its shape. Dynamic recognition (also called on-line recognition) involves an individual signing their name onto an electronic sensor pad. During this method, information relating to the pressure and velocity point of the stylus is recorded and analysed. Differing from the static mode, there is no need for the use of the optical scanners as the signature is already digitalised. Dynamic handwriting biometrics are more difficult to forge, as replicating the pressure and velocity in which the signature was originally produced can be more complex (Faundez-Zanuy 2006).

Static handwriting biometrics can be easily faked (Faundez-Zanuy 2005). Imposters can learn how to sign a name in the exact same way as another person. This can be done in one of three ways; simple forgery, substitution forgery or freehand forgery. Simple forgery occurs where the attacker traces over the original signature. Substitution forgery occurs when the forger substitutes the original signature with their own. This type of forgery works off the assumption that the signature will not be verified by the system. A freehand forgery occurs when the forger practises replicating the signature as close to the original as possible. This includes attempting to replicate the pressure and velocity that was used to create the original signature. It is this type of forgery that attempts to fool both static and dynamic signature biometric recognition systems (Hou et al. 2004).
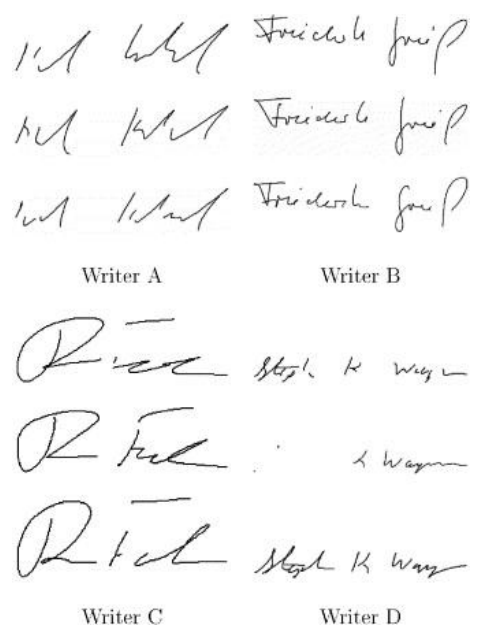


**Figure 34: Signature Variations (Anil K. Jain et al. 2002)**

A drawback to using handwriting recognition technology is that many people exhibit a large variance in letter shapes each time they sign their name, as shown in Figure 34. Factors like a person's posture, time constraints and signature habits that can cause these variations.

This issue can be resolved using a multi-modal enrolment approach. This approach requires users to input their signature multiple times. This way a large set of signatures variations can be recorded and analysed (Faundez-Zanuy 2005).

## 4.6 Ubiquitous Biometrics

Current biometric systems require a user to purposefully input their biometric information using specially designated biometric sensors. The concept of ubiquitous biometrics involves capturing an individual's biometric data without the user having to purposely interact with a biometric recognition sensor. These biometric sensors would be designed to gracefully integrate into a user's environment and any analysis of this data would be conducted by the computer system in the background.

Apple applied for a patent in 2005 that protects handheld devices, like the iPad and iPhone, with "touch sensors" (Apple Inc. 2005). These touch sensors are designed to take a pixelised image of a user's hand or fingerprint ubiquitously by the user simply holding the device, as illustrated in Figure 35 and Figure 36.
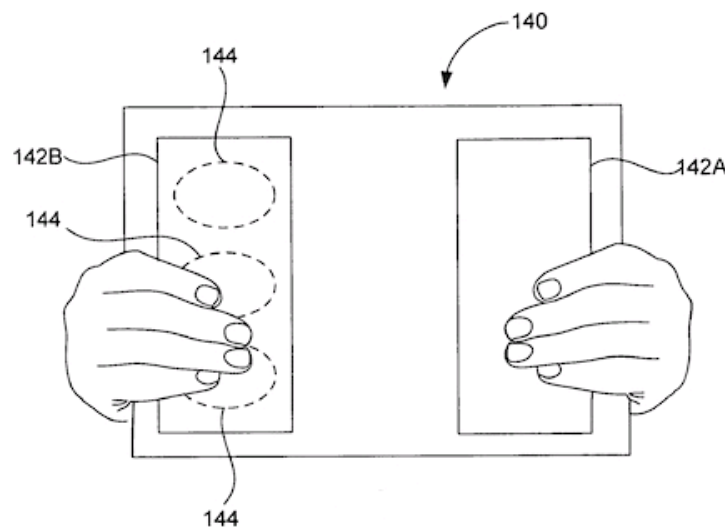


**Figure 35: Touch sensors on the back of the handheld device (Apple Inc. 2005)**
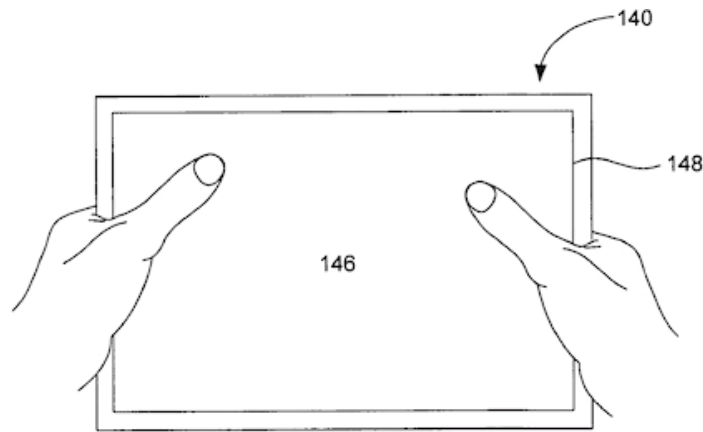
**Figure 36: Touch sensors on the front of the handheld device (Apple Inc. 2005)**

Once this biometric information is inputted it is stored in an image file on the device. This image file is then used to create a user profile and configure the device according to that user's preferences. The security of the biometric feature is not important in this implementation. It is the personal profiling capability that the feature is intended for. For example, if a family were to share one iPad device in a household, a family member could identify themselves to the device and apply their personal user preferences and customisation by simply picking the device up. This means that the children of the household could be blocked from using certain features on the iPad that are not suitable for their age group.

## *4.7 Conclusion*

A human's physiological and behavioural biometric scan be captured and examined in order to identify or verify a human to an authorisation system. Face recognition, fingerprint recognition and retina recognition are examples of physiological biometrics. Voice and handwriting recognition are examples of behavioural biometrics. A summary of these recognition methods are illustrated in Table 3.

**Table 3: Summary of Biometric Methods**

| Biometric | Type | Captured by | Usage |
|---|---|---|---|
| **Fingerprint** | Physiological | Fingerprint scanner | Criminal Trials |

| | | | |
|---|---|---|---|
| **Retina** | Physiological | Retina scanner | Electronic Passport |
| **Face** | Physiological | Camera | Passport Control |
| **Voice** | Behavioural | Sound Recorder | Telephone Services |
| **Handwriting** | Behavioural | Tablet | Bank Transactions |

Physiological biometrics are more secure than behavioural biometrics are they are subject to less change or forgery than behavioural biometrics.

Fingerprint and retina biometric recognition require proprietary hardware in order to capture the biometric data. However, face, voice and handwriting recognition can be captured using hardware that is readily available in the public domain via laptop, desktop, tablet and mobile phone computer systems.

# 5   METHODOLOGY

## 5.1  Introduction

Many design methods were selected to assist with the implementation of the BioScope application and with the collection of quantitative and qualitative data before and during the experiment. This chapter outlines these methods and provides a justification for the decisions that were made in the context of the experiment.

## 5.2  Survey and Interview Methodology

The experiment used two surveys and interview processes. The first survey was designed to collect information regarding CAPTCHA usage and user satisfaction. The second survey aimed to provide an understanding of social and privacy issues associated with the use of biometric recognition.

To ensure successful results from the use of these surveys a few factors were considered including distribution, response rate and the style of questions.

Firstly to incorporate the views and opinions from a wide range of individuals the survey was distributed in a format that promoted universal design. The target audience for the surveys were computer and Internet users with a broad range of skills and abilities. To ensure accessibility and flexibility in use, the survey was made available online (Selwyn & Robson 1998) and in paper format.

Web based surveys offer a convenient means to distribute a survey. There are two ways to conduct a web based survey. The first approach is to send a survey in an email and allow users to reply to this email with their response. The second approach is to use an online survey system and send a survey invitation to users via email. Email based surveys can have as low of a response rate as 20%, while email survey invitations can achieve a higher response rate (Andrews et al. 2003). In order to achieve as high of a response rate as possible an online survey system was used and invitations were sent via email and Facebook. Survey response rates can more than double when a reminder for the survey is distributed (Kittleson 1997), therefore

following the initial broadcast of the survey in the experiment, a reminder was sent out a week later to participants.

The design of the survey and its questions can also affect a survey's response rate. Some research has shown that shorter surveys perform better than longer surveys (Sheehan 2001). This factor was incorporated into the surveys by ensuring that each questionnaire contained 5 or less questions.

The questions in the surveys aimed to produce numerical statistical information relating to CAPTCHA and biometric usage. To collect this type of data, closed ended question styles, which could be answered with true or false values, were used in the survey. To explore this quantitative data further, the same questions asked in the survey formed the basis for an unstructured interview process. The interview questions were designed to collect qualitative data regarding CAPTCHA and biometric usage.

## 5.3  Development Methodology

When designing, implementing and evaluation an accessible and usable software application, it is important to use a user centric development methodology. The *Star Lifecycle Model* focuses on user evaluations at each stage of development, as illustrated in Figure 37. Using this model ensures that usability and accessibility is considered throughout the development process (Hix & Hartson 1993).
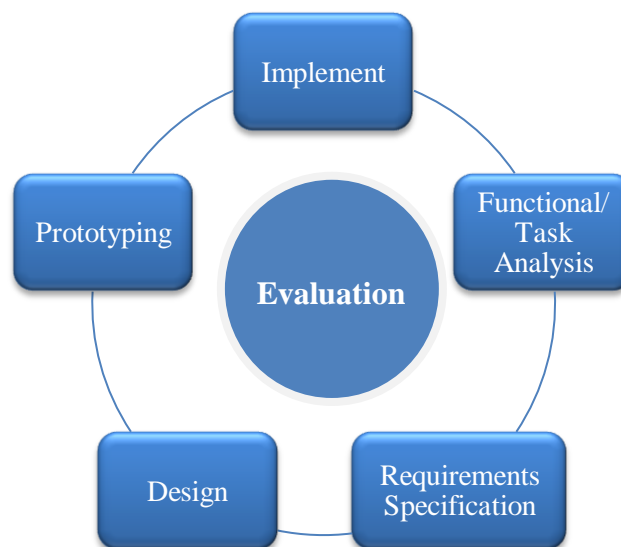


**Figure 37: Star Lifecycle Methodology**

The *Star Lifecycle Model* has 6 phases that need to be addressed during product development. A unique aspect to this software life cycle is that it does not work on a top down direction like traditional waterfall methodologies. Instead the life cycle can start at any point and in any order (Costabile 2001):

**Phase 1**: In the task and functional analysis phase the overall goals of the system and the user needs were identified. In the experiment the ICF framework was used during this phase to determine what combination of biometric recognition methods should be offered by the system.

**Phase 2:** The requirement phase involved gathering information regarding what the user needed from the system. These requirements were gathered based on the literature review.

**Phase 3:** The conceptual and functional design phase concentrated on outlining how the system would work. During this phase in the experiment heuristic evaluations were conducted to ensure the diverse needs of users were met (Lang 2003).

**Phase 4:** The user interface design was explored during the prototyping phase. Low, medium and high fidelity prototyping are equally as good at finding usability issues, however all types uncover different levels of feedback from users. For this reason all three prototyping methods were used as part of the application development.

**Phase 5**: The product was finally developed during the implementation phase.

**Phase 6:** The evaluation phase was the most important aspect to this methodology. User testing and literature evaluations were conducted after every phase of the life cycle model.

## 5.4  Evaluation Methodology

The aim of the evaluations was to establish how accessible and usable the BioScope's user interface was compared to the reCAPTCHA's user interface. reCAPTCHA was chosen as the baseline CAPTCHA test for two reasons. Firstly reCAPTCHA is

considered the industry standard for CAPTCHA applications. Secondly, in comparison to the other CAPTCHAs, reCAPTCHA's text based tests have a higher human pass rate than any other.

This evaluation was conducted using *usable accessibility* measurements, as outlined in Section 2.8. This method involved collecting usability data from a diverse group of testers with varying skills, abilities and disabilities.

To determine if each application was accessible, 10 users with different skills, abilities and disabilities were selected to test the applications (W3C 2010). Any issues or failures found during this testing indicated that the user interface was not accessible. In the past it was widely considered that 5 testers were suitable to find the majority of software bugs (Nielsen 2000). However it has been shown by Faulkner that 5 testers only uncover 55% of the issues in a software system. 10 testers ensure 80% of issues in the software are found. 20 testers find 95% of the issues (Faulkner 2003) (O'Connor 2011).

To establish if each application was usable, quantitative and qualitative data was collected regarding the 5 usability characteristics: **learnability**, **memorability**, **efficiency**, **errors** and **user satisfaction** (Nielsen 2003). Learnability, memorability and efficiency of each application was determined by the time in which it took a user to complete the various tasks involved with both the reCAPTCHA and the BioScope user interface. As BioScope did not have any back-end server or validation processes, the times recorded for both reCAPTCHA and BioScope started from when the user opened the application and ended when they pressed the submit button. This meant that any time taken up by validation or error messages following this submission event were not included in the time results. Users were asked to repeat each test three times. If the users were able to decrease the time in which it took them to use the application after each attempt, this indicated that the application was **learnable** and **memorable**.

The **efficiency** of the application was determined by how quickly each user could complete a task (Nielsen 2003). The **error** usability factor was determined by recording how many failures occurred during each test. As the BioScope application did not have any way to determine whether the biometric information supplied was

correct or not, an error in BioScope was recorded when a user did not follow the instructions displayed in the user interface correctly.

**User satisfaction** was determined by conducting a SUMI survey and analysing the qualitative data that was collected. A SUMI questionnaire is designed to establish user satisfaction when using a software application. Each SUMI questionnaire has 50 questions and takes approximately 10 minutes to complete (Arh & Blažič 2008). See Section 2.8.2 for more information regarding the SUMI questionnaire.

## 5.5 Conclusion

This chapter outlines the methodologies that were used in the context of the experiment. This includes the methodologies used for the survey design, BioScope's design and the evaluation design.

The survey methodology focused on three areas; distribution, response rate and question styles. An accessible distribution process was implemented by providing the survey in multiple forms (paper and online). This ensured a wide range of individuals could participate in the survey. To encourage a large response rate, social networking sites and follow up notifications were used to inform people about the survey and encourage them to complete it. The survey was designed to collect quantitative data by using closed ended structured questions. To follow up on these results and explore some of the survey topics further an unstructured interview was conducted to collect qualitative and quantitative data regarding CAPTCHA and biometric usage.

The *Star Lifecycle Model* development methodology was used to implement the BioScope application. This methodology is a user centric development methodology that promotes usability and accessibility by conducting user evaluations following each phase of development.

Finally, the evaluation methodology focuses on *usable accessibility* measurements. This means that the five usability measurements outlined by Nielsen (efficiency, learnability, memorability, failure rate and user satisfaction) were used to collect data during the diverse user testing.

# 6 EXPERIMENT

## *6.1 Introduction*

In the previous three chapters relevant information has been identified and reviewed in the context of the experiment, as illustrated in Figure 38. Chapter 2 reviewed literature in the accessibility and assistive technology fields and provided an understanding of the issues faced by individuals with disabilities. Chapter 3 identified the different CAPTCHA tests that are currently available on the market and outlined their weaknesses and limitations. Chapter 4 investigated the different types of biometric recognition that are currently available and identified social concerns with their use.
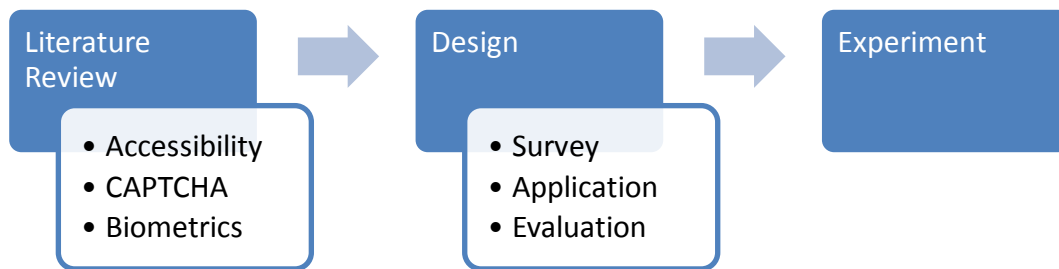


**Figure 38: Experiment Process**

This chapter provides a review of the design decisions that were made when implementing the BioScope software, describes how the experiment was conducted and discusses the testing that was involved.

## *6.2 Survey Design*

### 6.2.1 CAPTCHA Survey

To gain an understanding of CAPTCHA's usage and its popularity in the public domain a survey was conducted as part of the project. The results of this survey illustrated whether an accessible alternative to CAPTCHA was needed. In total, 70 surveys were completed. The electronic survey was distributed via email and Facebook and the paper format was hand delivered. This broad distribution of the survey allowed

for data collection among a large variety of computer user's with different skills and abilities.

## 6.2.2  Biometric Survey

As discussed in Section 4.3 privacy is an important aspect that needs to be considered with any biometric recognition system. Protecting people's biometric data is paramount as, unlike passwords or smartcards; biometric information that is compromised cannot be reissued or revoked (A. K. Jain et al. 2008).

Considering this, individuals may be more hesitant to supply their biometric information to various organisations. To understand this point more, a social acceptance and privacy survey was conducted as part of this project. This survey focused on user's acceptance and comfort levels with supplying their biometric data to online services. The results of this survey were designed to illustrate whether a biometric alternative to CAPTCHA would be accepted by users. If deemed not acceptable, user satisfaction levels could be negatively affected when using a biometric user interface like BioScope.

The electronic survey was distributed via email and Facebook and the paper format was hand delivered. This broad distribution of the survey allowed for data collection among a large variety of computer user's with different skills and abilities. In total, 70 surveys were completed. To explore the survey's topics further, the same questions were asked in an interview process. This allowed participants to expand on their thoughts relating to security, privacy and biometric recognition services. In total, 10 interviews were completed.

## *6.3  Functional Analysis*

Chapter 2 established that CAPTCHA is used to prevent *n* number of bots from accessing online resources while still allowing access for humans. While the CAPTCHA has some success in preventing bots, it can prevent many users with disabilities from accessing these resources. The aim of this project was to create an accessible CAPTCHA user interface. This user interface was designed to acquire biometric data from an individual to allow for an online system to create a unique user

account. This in turn would prevent *n* number of bots from creating *n* number of accounts. The developed system, named BioScope, focused solely on capturing this biometric data in an accessible and usable manner.

## 6.4 Interaction Requirements

Before development could begin on the user interface, the biometric recognition methods that would capture an individual's data needed to be selected. All human abilities, skill levels and disabilities were considered with each biometric selection. This ensured the system was accessible and considerate for each user. There were three aspects that were taken into account when selecting the appropriated biometric recognition interactions.

The first aspect to consider was the technical requirements of the system. The World Wide Web Consortium (W3C) suggested that a biometric alternative to CAPTCHA would be implemented in conjunction with a single sign-on logon account (W3C 2005). A single sign on service would require that the captured biometric data could be used to uniquely identify an individual.

In general, biometric data can be used to identify a human or an individual. For example, thermal biometric recognition can identity that an individual is human, but cannot uniquely identify the individual. In contrast, face biometric recognition can identify that an individual is human as well as identifying who the individual is. Considering this, it was concluded that not all biometric recognition types were valid for this approach; see Table 4 for more information.

**Table 4: Identifying a Human vs. an Individual**

| IDENTIFY A HUMAN | IDENTIFY AN INDIVIDUAL |
|---|---|
| Face | Face |
| Voice | Voice |
| Gesture | Handwriting |
| Handwriting | Iris |

| | |
|---|---|
| Iris<br><br>Retina<br><br>Fingerprint<br><br>Vascular Scan<br><br>Thermal<br><br>DNA | Retina<br><br>Fingerprint<br><br>Vascular Scan<br><br>DNA |

The second aspect to take into account was the biometric recognition limitations of the iPad. The iPad comes with a multi-touch screen, a forward and backward facing camera, microphone and built-in speakers (Apple Inc. 2012). Therefore, biometric types that could not be accurately recorded using the iPad hardware could not be used in the software implementation, See Table 5 for a breakdown of the iPad's biometric recognition capabilities.

**Table 5: iPad Biometric Recognition Capabilities**

| Can be recorded using iPad | Cannot be recorded using iPad |
|---|---|
| Face<br><br>Voice<br><br>Handwriting | Iris<br><br>Retina<br><br>Fingerprints<br><br>Vascular Scan<br><br>Handprint<br><br>Thermal<br><br>DNA |

The last aspect to consider was that the biometric recognition methods chosen needed to be accessible for as many users as possible. If one biometric recognition method was not accessible to a particular user group, then an accessible alternative for this user

group needed to be available in the user interface. The ICF was used to indicate what groups of users may have a problem using each biometric recognition method, as illustrated in Table 6.

The ICF indicated that the face and handwriting recognition tasks were inaccessible for users who had visual impairments and hand/arm mobility impairments. In terms of the face recognition, these users might have difficulty in positioning the iPad correctly so that their face was located in the camera's viewpoint. For the handwriting task, these user groups might have difficulty with producing an accurate representation of their personal signature. Taking these user groups into consideration, the ICF indicated that the voice recognition task would act as an accessible alternative.

The voice recognition task was deemed inaccessible for individuals with voice/speech and respiration difficulties. As an alternative, the ICF indicated that the handwriting recognition task was an accessible alternative.

The ICF also indicated that the face recognition task and the handwriting recognition task would not be accessible for users with visual impairment. For these users, the voice recognition task acted as an accessible alternative.

**Table 6: ICF Considerations for Biometric Selection**

| FUNCTIONS | FACE | VOICE | HAND WRITING |
|---|---|---|---|
| Consciousness | Inaccessible | Inaccessible | Inaccessible |
| Intellectual | Accessible | Inaccessible | Inaccessible |
| Seeing | Inaccessible | Accessible | Inaccessible |
| Orientation | Accessible | Inaccessible | Accessible |
| Language | Inaccessible | Accessible | Accessible |
| Voice | Accessible | Inaccessible | Accessible |
| Involuntary Movements | Inaccessible | Accessible | Inaccessible |
| Mobility in Joints | Inaccessible | Accessible | Inaccessible |
| Muscle Power | Inaccessible | Accessible | Inaccessible |

| | | | |
|---|---|---|---|
| Perceptual | Accessible | Accessible | Accessible |
| Skin | Accessible | Accessible | Accessible |
| Respiration | Inaccessible | Inaccessible | Accessible |
| **STRUCTURE** | **FACE** | **VOICE** | **HAND WRITING** |
| Brain | Inaccessible | Inaccessible | Inaccessible |
| Ear, Eye Structures | Inaccessible | Accessible | Inaccessible |
| Voice and speech | Accessible | Inaccessible | Accessible |
| Spinal Cord | Inaccessible | Accessible | Inaccessible |
| Head movement | Inaccessible | Accessible | Accessible |
| Arm, hand movements | Inaccessible | Accessible | Inaccessible |
| Respiratory Systems | Accessible | Inaccessible | Accessible |
| **ACTIVITY & PARTICIPATION** | **FACE** | **VOICE** | **HAND WRITING** |
| Watching | Inaccessible | Accessible | Accessible |
| Lifting and carrying | Inaccessible | Accessible | Accessible |
| Fine hand use | Inaccessible | Accessible | Accessible |
| Communication Systems | Accessible | Inaccessible | Accessible |
| Speaking | Accessible | Inaccessible | Accessible |
| Learning to read | Accessible | Accessible | Accessible |
| Learning to write | Accessible | Accessible | Inaccessible |
| **ENVIRONMENTAL** | **FACE** | **VOICE** | **HAND WRITING** |
| Light | Inaccessible | Accessible | Accessible |
| Sound | Accessible | Inaccessible | Accessible |

To allow us to quantify these user groups, the Exclusion Calculator was used. As discussed earlier in Section 2.7.2, the Exclusion Calculator is mapped to UK census statistics. To allow us to measure what these exclusion indications meant for the Irish population, results were mapped against the Irish census statistics (Central Statistics Office 2007).

The chart in Figure 39 illustrates the number of individuals in the UK and Ireland that would have difficulty using handwriting recognition. In total, 8.4% of the UK's population and 3.4% of Ireland's population would be unable to use handwriting recognition.

**Exclusion Calculator - Handwriting Task**

UK  Ireland

Vision: UK 3.4%, Ireland 1.1%
Hearing: 0.0% 0.0%
Thinking: 0.0% 0.0%
Dexterity: UK 5.0%, Ireland 2.3%
Reach and Stretch: 0.0% 0.0%
Locomotion: 0.0% 0.0%
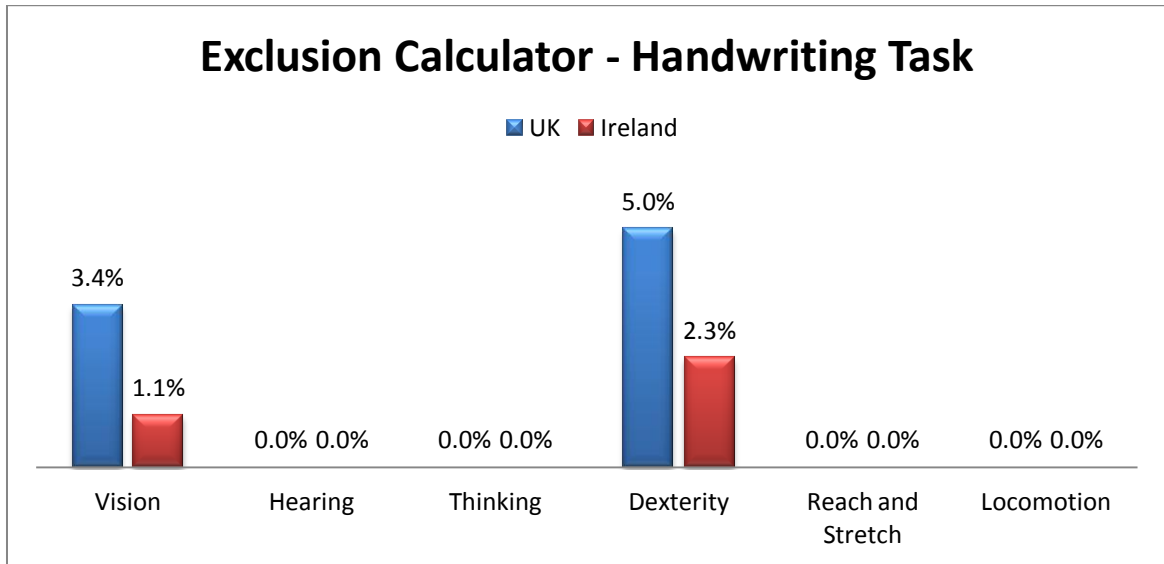
**Figure 39: Exclusion Calculator Results for Handwriting Task**

The chart in Figure 40 shows the percentage of the population in the UK and Ireland that would have difficulty with using voice recognition. These results indicate that a voice recognition task should be inaccessible for 0.9% of the UK population and 1.3% of the Irish population.

**Exclusion Calculator - Voice Task**

UK  Ireland

Vision: 0.0% 0.0%
Hearing: UK 0.9%, Ireland 1.3%
Thinking: 0.0% 0.0%
Dexterity: 0.0% 0.0%
Reach and Stretch: 0.0% 0.0%
Locomotion: 0.0% 0.0%
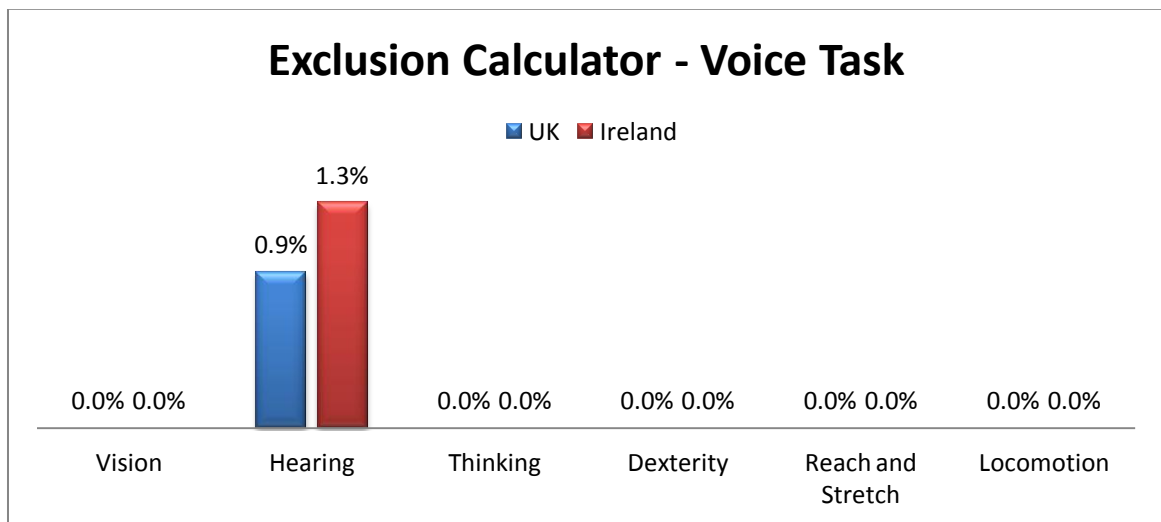
**Figure 40: Exclusion Calculator Results for Voice Recognition**

The chart in Figure 41 represents the percentage of individuals living in the UK and Ireland that would be unable to complete a face recognition task. In total, 5.1% of the UK's population and 3.45 of the Irish population would find this task inaccessible.
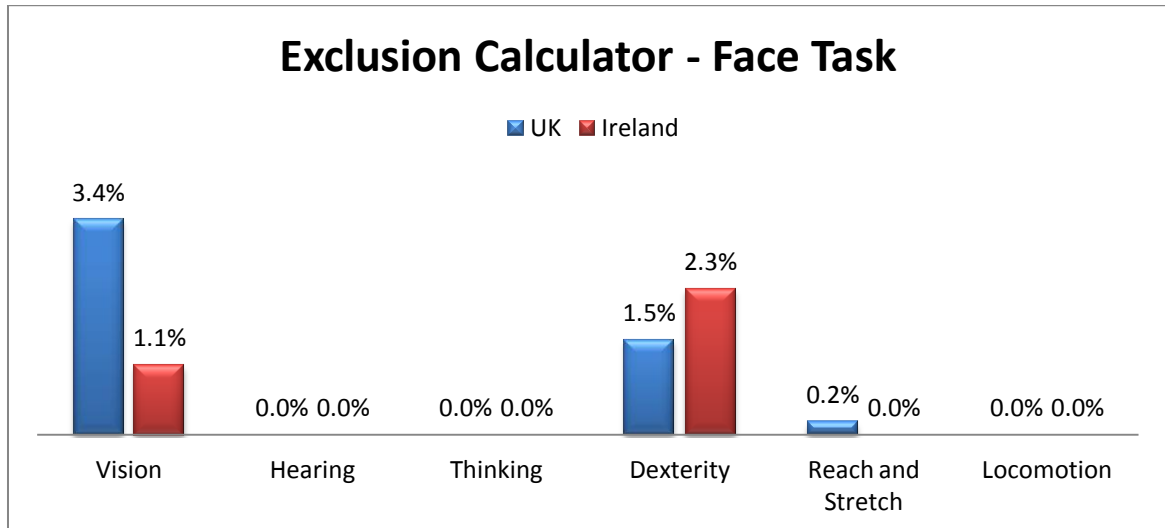


**Figure 41: Exclusion Calculator Results for Face Recognition**

To summarise, these results from the Exclusion Calculator show that at least one of the biometric methods would be accessible to users irrespective of their disabilities. In contrast, CAPTCHA does not offer the same accessible combinations.
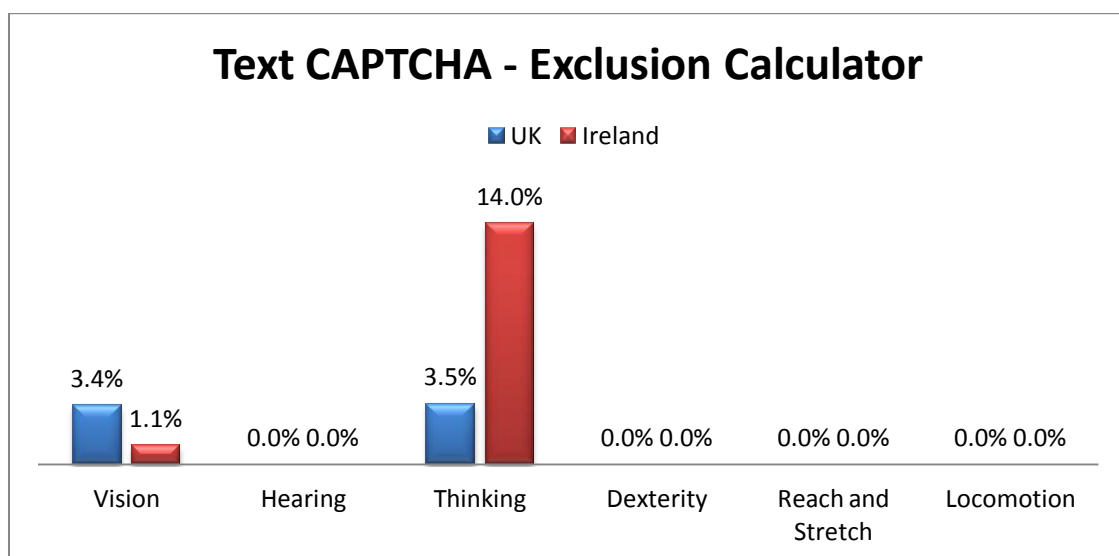


**Figure 42: Text CAPTCHA - Exclusion Calculator**

CAPTCHA system can directly affect people with reading and writing difficulties whether a text based CAPTCHA is used or an audio based CAPTCHA, as illustrated in Figure 42 and Figure 43. According to the 1996 International Adult Literacy Survey (IASL) Ireland has a high illiteracy rate of 25% (NALA 1997).
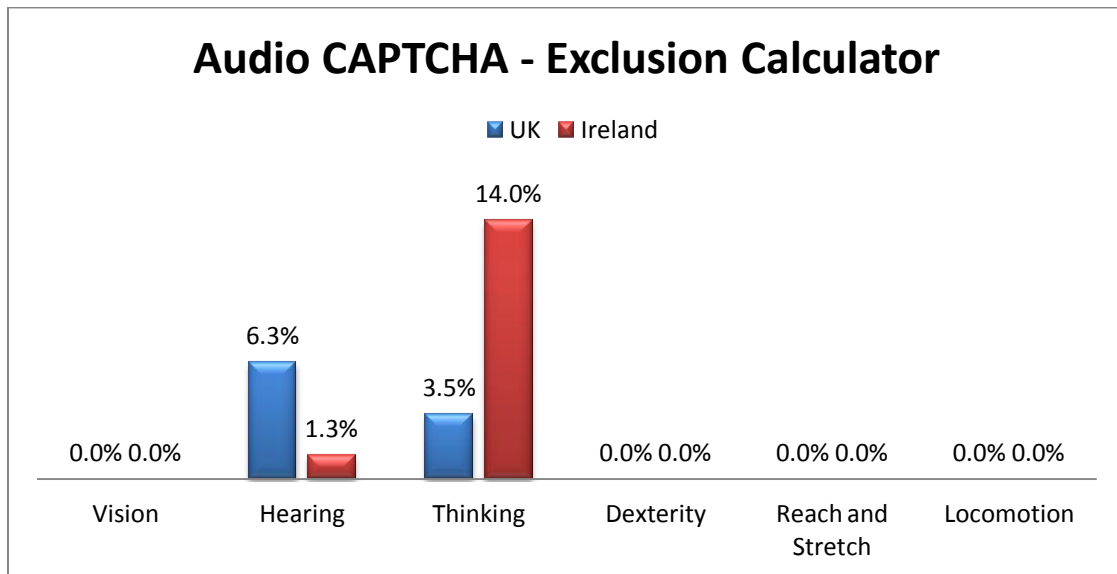


**Figure 43: Audio CAPTCHA - Exclusion Calculator**

Designing the BioScope system to use face recognition, voice recognition and handwriting recognition ensured that, unlike the CAPTCHA interface, the BioScope could accurately record all necessary data, each individual could be uniquely identified using this data and the interaction would be accessible to as a wide a range of users as possible.

## 6.5 Task Analysis

In the previous section the three biometric recognition methods used in the BioScope system were established; Handwriting, voice and face recognition. With this, a user interface was designed for each biometric data capturing task.

The handwriting task asked the user to sign their name using the iPad's touch screen capabilities. The face recognition task required that a user positioned there face correctly in the camera's view point, and once their face was recognised (indicated by

a red square that displayed around the individual's face on screen) the user captured a picture of their face. The voice recognition task required that users recorded themselves reading words that appeared on the iPad screen aloud. Blind users would be required to use a screen reader to read the words that appeared on the screen, see Figure 44. Blind users were required to access their short term memory and recall the words aloud. Miller states that users can recall a maximum of 7+/- 2 chunks of information at a time without difficulty (Miller 1956). For this reason it was decided to present a user with 5 words for each task.



**Figure 44: BioScope's Voice Recognition Task**

## 6.6 Formal Design

Each biometric recognition task was designed to be accessible and usable. This was achieved by using industry standard guidelines and principles.

*Apple's User Experience Guidelines* were considered to ensure that the BioScope application was consistent with other iPad applications on the market. These guidelines also take into account how a user interacts and behaves with an iPad device and thus

suggests techniques to increase usability in an application. See Section 2.6.2 for more information on these guidelines.

The Universal Design Principles were also considered when designing BioScope. These principles ensure that the application was as accessible to as wide a range of individuals as possible. See Section 2.6.3 for more information on these principles.

## 6.6.1   User Interface Controls

The *Apple's User Experience Guideline* explains that important user interface controls and information should be made obvious to the user (*Elevate the Content that People Care About*). In keeping with this guideline, controls in the BioScope application that were no longer needed by the user were greyed out and disabled to allow a user to focus on the controls that were relevant for completing the task at hand. For example, on the voice recognition screen, the record control was disabled once a user had already begun to record their voice. This allowed the user to focus on the next step of the test which was to use the stop control. This is illustrated in Figure 45.



**Figure 45: Emphasising the Record Button**

To ensure that the BioScope application was intuitive to use, only user interface controls and behaviours that were consistent with other iPad applications were used, as documented in the *iOS UI Element Usage Guidelines*  and Apple's *User Experience Guidelines* (Apple Inc. 2010). For example, all controls that submitted or confirmed information were highlighted using Apple's "*done*" colour scheme (Blue button with white text). This indicated to each user the importance and function of this control. See Figure 46 for an example of this user interface design technique.

**Figure 46: Navigation Design**

Another technique implemented to ensure consistency, was the positioning of navigational elements and page controls. In line with the Apple guidelines, any navigation control that allowed a user to move from screen to screen was placed in a navigation bar at the top of the screen. Any control that interacted with the currently displayed screen was placed in a toolbar at the bottom of the screen. For example, all back and next buttons were placed in a navigation bar at the top of each screen and a page control like the photo capture button was correctly placed at the bottom of the screen in a toolbar.

To ensure a logical navigation path was presented to the user (as outlined in Apple's guideline *Give People a Logical Path to Follow*) the BioScope application used a back button on every screen in the application. This technique ensures that users know where they are in the application and how they can retrace their steps. To allow BioScope to adhere to this guideline only one navigational path was available to a user when using the BioScope user interface. A simple navigation and page hierarchy system are maintained throughout.

## 6.6.2   User Preferences

Apple state in their guideline *De-emphasis Settings*, that the use of settings and user preference should be discouraged for an application. If an application is designed to function in a predictable and effective way, a user should never need to adjust the application's behaviour. An initial concept for the BioScope application was to allow screen reader users to adjust the application's settings which would offer them a different set of biometric recognition methods and tasks. However, after considering the guidelines this approach was deemed incorrect. Instead the screens were designed for all users universally and worked the same whether a user was using a screen reader or not. This approach also incorporated the *Universal Design Principle of Equitable Use* by ensuring that all menu items and screens were designed to operate in the same

way whether a user was using the iPad in standard mode, screen reader mode or switch mode.

This approach also fell in line with the *Universal Design Principle of Flexibility in Use*. The BioScope application accommodated a wide range of user's abilities and preferences. If a user selected to use the face recognition method they could choose whether to use the front facing or back facing camera, as illustrated in Figure 47.
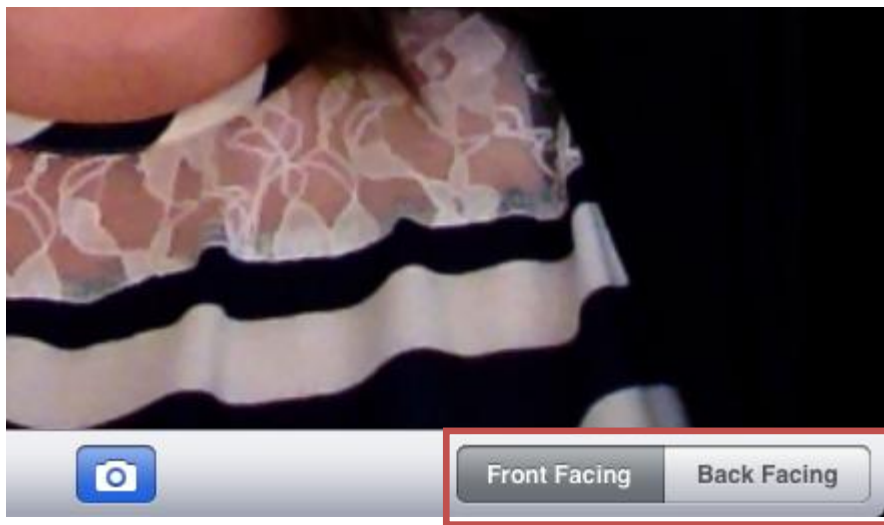


**Figure 47: Front or Back Facing Camera Choice**

In terms of differences in a user's vision, Users could zoom in on the user interface using the pinch-to-zoom gesture on the iPad if they found that the text instructions and labels on the screen were too difficult to read. When this was done, all the information and images in the BioScope application were correctly resized for the user. This feature also benefited users with accuracy and precision difficulties as all controls became larger on iPad screen once zoomed in. This meant that users could press the appropriate buttons with greater ease.

**Figure 48: Imagery Used in BioScope**

### 6.6.3 Text and Imagery

Short labels, symbols and meaningful imagery were used throughout the BioScope application to ensure the user interface was succinct. The main screen controls were accompanied with relevant imagery. This is illustrated in Figure 48. The camera controls on the face recognition input screen also used symbolism to indicate to a user what control should be pressed in order to take a picture of their face, Figure 49.



**Figure 49: Camera Symbol**

### 6.6.4 Data Collection

Apple indicates in their guideline *Make Modal Tasks Occasional and Simple* that modals should be used when it is critical to get a user's attention and when a task involving a user's data must be completed. For this reason, the BioScope application was designed to display a confirmation modal to a user once the biometric recognition task was complete, see Figure 50. This allowed a user to review all data submitted, ensure the information was correct and then complete the task.
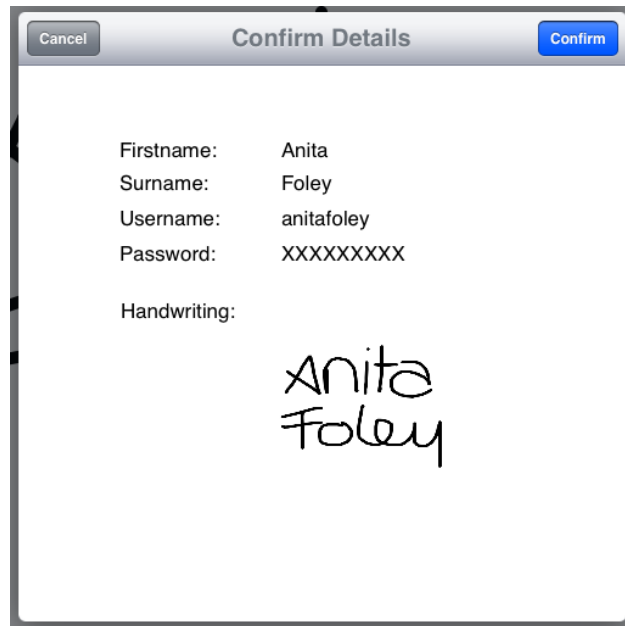
**Figure 50: Confirmation Modal in BioScope**

The universal principle of *Tolerance for Error* was carefully considered when designing the BioScope application. Rather than providing the user with error and validation messages, the BioScope application aimed to prevent users from causing any errors in the first place. All hazardous actions and errors were avoided by disabling controls that were no longer necessary for the completion of each task. For example, a user could press the record button when providing the BioScope system with their voice information. To ensure the user did not interrupt this process once the recording had begun, the record control was disabled, see Figure 45 for an illustration of this. This control was only re-enabled after the user had indicated in the confirmation modal that the voice information provided was not correct. Similarly, the camera button on the face recognition screen was also disabled once users had taken a correct image of themselves to prevent them deleting the previously taken photograph.

## 6.7 Prototyping and Implementation

All the considerations outlined in the design phase were implemented during the prototyping stage. During the process, user acceptance testing and interviews were conducted to ensure the needs of each user had been correctly considered. Following each prototype, the results collected from each evaluation cycle were used to improve the next set of prototypes.

### 6.7.1 Low fidelity

The first version of the software was implemented using a paper prototype. This allowed for the collection of important user input and opinions without needing to invest a large amount of time, effort or money into its development.

The initial version of the prototype presented the user with three biometric recognition options. Following the selection of a preferred recognition method, the user was presented with the chosen biometric recognition task, as illustrated in Figure 51.



**Figure 51: Paper Prototype of BioScope's Main Screen**

Following user's evaluations of this prototype, it was determined that the screens were easy to follow and understand. Users felt that the text information was clear and that the screens were not overly complex or cluttered. Given the success of the paper prototype, the BioScope application was implemented using a medium fidelity prototype.

### 6.7.2 Medium fidelity

The medium fidelity prototype was developed using a prototype tool on the iPad called *Blueprint* (Groosoft 2012). This tool generated iPad application controls that were styled consistently with other iPad applications, see Figure 52. Once the controls were generated each application screen could be previewed. This meant that testers could interact with the prototype using standard iPad tapping and gesture recognition. This prototype identified any remaining issues with the design of the application's user interface which were, in turn, removed in the high fidelity prototype.

**Figure 52: Medium Fidelity BioScope Prototype**

### 6.7.3   High Fidelity

Following the completion of both the low and medium fidelity prototypes, development began on BioScope high fidelity prototype. The application was designed to capture a user's biometric information and store it on the iPad. The application was developed using the Objective C programming language. Apple's Integrated Development Environment *Xcode* was the development tool used in this process.

## *6.8   Evaluation*

10 users with different skills, abilities and disabilities were selected to test the applications (W3C 2010), shown in Table 7.

**Table 7: Application Tester's Profiles**

| Tester Name | Tester Profile |
|-------------|----------------|
| Tester A | 63 year old<br>Female<br>Computer Novice |
| Tester B | 65 year old<br>Male<br>Computer Novice |
| Tester C | 27 year old<br>Male |

| | |
|---|---|
| | Colour Vision Limitations<br><br>Computer Expert |
| Tester D | 25 year old<br><br>Female<br><br>Computer Intermediate<br><br>Used Headphones |
| Tester E | 24 year old<br><br>Male<br><br>Computer Expert<br><br>English is not first language |
| Tester F | 34 year old<br><br>Male<br><br>Computer Expert<br><br>Dyslexic |
| Tester G | 54 year old<br><br>Female<br><br>Computer Intermediate |
| Tester H | 35 year old<br><br>Male<br><br>Computer Expert<br><br>Broken Elbow |
| Tester I | 29 year old<br><br>Female<br><br>Computer Intermediate<br><br>Arthritis |
| Tester J | 30 – 40 years old<br><br>Male<br><br>Computer Expert<br><br>Blind<br><br>Used Headphones |

Each tester was given an iPad and a set of headphones to conduct the testing. Only 2 of the10 testers availed of the headphones. As described in Section 5.4, testing times were

recorded when testing both the reCAPTCHA system and the BioScope system. These results indicated if the system was learnable, memorable and efficient. The failure rates were recorded to establish if the system was error prone. Finally a SUMI user satisfaction survey was conducted to determine if users preferred using the reCAPTCHA system or the BioScope system.

## 6.9 Conclusion

This chapter outlines how the software for the experiment was designed using both the *Apple User Experience Guidelines* and the *Universal Design Principles*. It discusses how BioScope was implemented using a user centric based prototyping methodology. The chapter concludes by discussing the experiment testing design in terms of tester selection and the measurements used to examine the usability and accessibility of the BioScope's user interface.

# 7    RESULTS AND ANALYSIS

## 7.1  Introduction

In the previous chapter the experiment was outlined including the software design, software implementation and the testing process. This chapter analyses and compares the results that were collected during this experiment with two key factors in mind. Firstly the analysis aims to determine if the BioScope application is more user-friendly and accessible than the CAPTCHA user interface and.  Secondly the evaluations aim to uncover if the design and testing methodologies used for the experiment assisted with creation of this accessible and usable user interface.

## 7.2  Survey Results

### 7.2.1   CAPTCHA Survey

In Figure 53 participants were asked if they had ever used CAPTCHA before. To ensure participants understood what a CAPTCHA was the term CAPTCHA was explained in the survey as a *"test that presents you with a picture of distorted letters and asks you to type in the letter sequence into an input field provided"*.
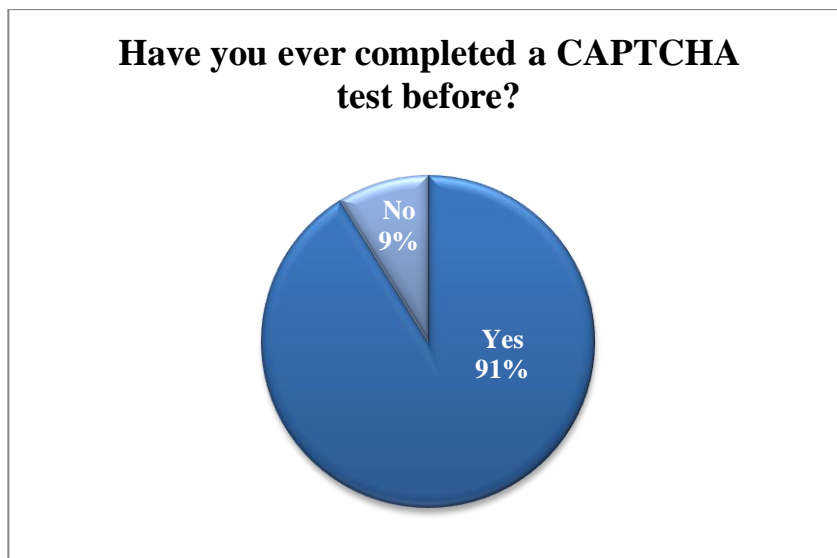


**Figure 53: Past Experience with CAPTCHA**

In total, 91% of the 70 people surveyed had used CAPTCHA previously. Of those 91%, 78% of participants had previously used CAPTCHA when buying a ticket for an event. Ireland's leading online ticketing company Ticketmaster Inc. ask users to complete a CAPTCHA before they can purchase a ticket on their site (Ticketmaster Inc. 2012). Another common Internet activity (71%) that involved the use of CAPTCHA was when creating a user account. E-mail service providers like Google force users to complete a CAPTCHA when creating a new Google account. 50% of interviewees stating that they had used CAPCHA when buying airline tickets online. These results are illustrated in Figure 54.
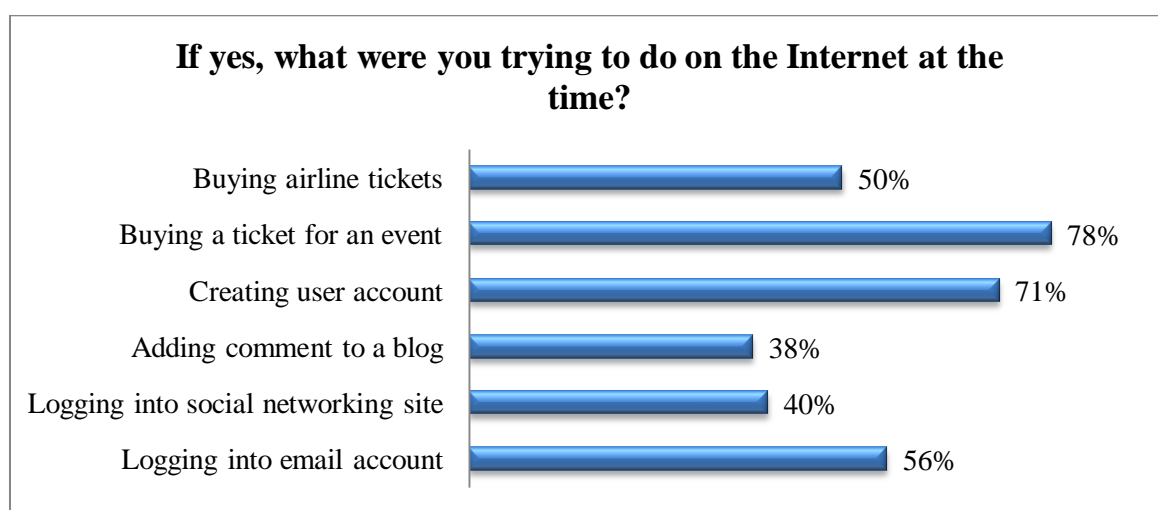


**Figure 54: Common CAPTCHA usage on the Internet**

Following this question, participants in the survey and interview were asked to add some comments relating to their experience with CAPTCHA. Participants who answered this question stated that they found CAPTCHA difficult to use and therefore didn't like it:

*"Many are really awkward to read. In such cases they are an unwanted hindrance and show a lack of consideration for the user".*

*"So annoying. Don't like them at all. I very often get them wrong".*

*"Generally I require at least one refresh before I can successfully complete it. They are annoying and occasionally have discouraged me from proceeding".*

## 7.2.2 Social Acceptance and Privacy in Biometrics Survey

The survey and interview participants were asked if they would give permission for a private (Google) or public (the Government) organisations to collect and store their biometric information. The results of this survey and interview are illustrated in Figure 55.



**Would you be comfortable with the Government/Google storing your biometric data?**

| | Fingerprint | Voice | Face | Retina | Handwriting |
|---|---|---|---|---|---|
| Google | 23% | 35% | 31% | 27% | 26% |
| The Government | 26% | 33% | 35% | 30% | 36% |
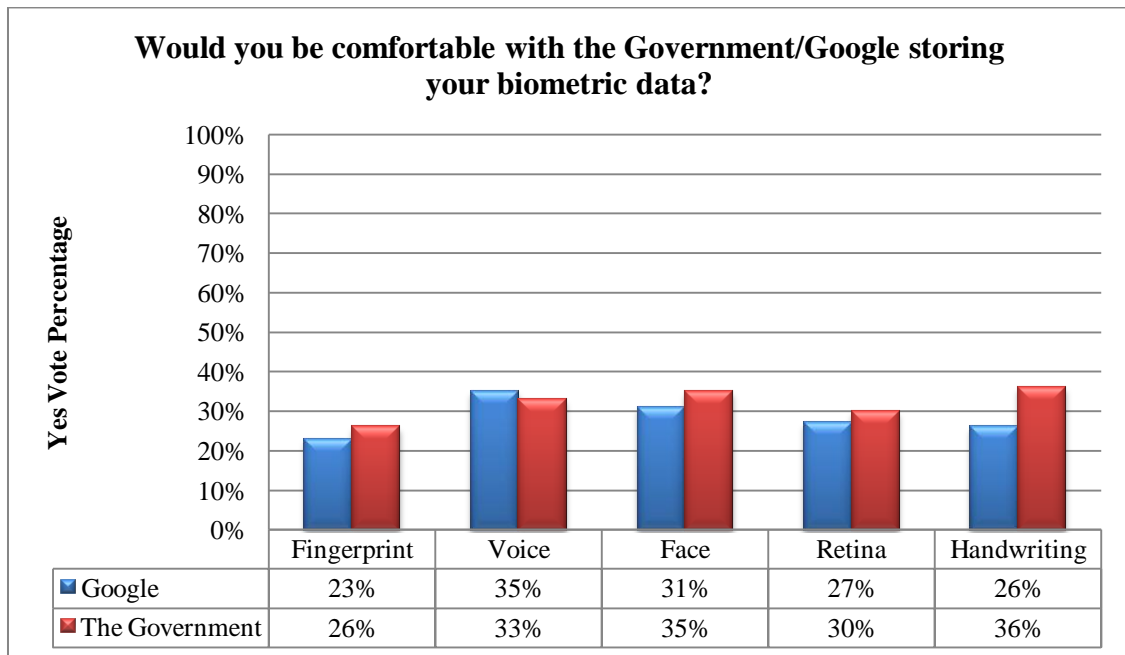
**Figure 55: Biometric Social Acceptance and Privacy Survey Results**

On average 26% of the all the participants were comfortable giving their fingerprint information to the Government. 23% of participants were comfortable with giving their fingerprint information to the Google. One interviewee stated:

> *"I think your fingerprint is very unique to you and it would be very difficult to deny your fingerprint. Well, it would be impossible to deny it. You'd find that Google would build up a pretty interesting profile about you. They'd know your personal and private information. So no, I wouldn't be keen on them having my fingerprint."*

Another interviewee reflected on their security and identity theft concerns:

*"Anything that's kept in a file format by someone can be hacked, and it's not that I think Google would misuse it, I just don't think they could keep it secure. If someone really wanted it they could get it... Government agencies especially. I mean you hear lads losing laptops that have private customer information on it. I wouldn't be happy with anyone having that information. Someone could pretend to be me."*

Any interviewee that expressed concerns relating to the Government storing their fingerprint were asked if they had ever used a fingerprint scanner in the airport when travelling to the United States. To enter this country it is mandatory for travellers to provide their fingerprint at the point of entry to the country. The purpose of this question was to understand why a person would give their fingerprint information to the Government in this scenario, but would not give the same information to a Government website. Some participants, although unhappy with giving their fingerprint information to immigration, would not give up the opportunity to fly to the United States. They felt it was a sacrifice they were willing to make.

*"I can do without Gmail, but if I have to go to the States, then I have to go to the States. It depends on leverage. My morals have leverage and to be fair, when it gets to Government rules I don't really have a choice."*

*"I don't have a choice. I mean, I want to go to the States and see my family, so I have to give them my fingerprint. But I don't have to use Gmail. I could just use hotmail or something."*

An average of 33% of the participants indicated that they would be happy with the Government storing their voice information and an average of 35% were happy for Google to store this information. From the interview conducted a few interviewees felt that a voice recognition system could not uniquely identify an individual as well as a fingerprint recognition system could and so therefore were happy to give both the Government and Google their voice information.

*"I think it's just not as personal. Fingerprint is so unique. You're giving away a piece of yourself. But the voice is less unique."*

> *"I wouldn't be as against the voice as the fingerprint. Your fingerprint is your fingerprint. You could change your voice, but you can't change your fingerprint."*

One interviewee who was not happy to give either the Government or Google his voice biometric information stated:

> *"I wouldn't be happy with them having any information in a digital format that could uniquely identify me".*

Regarding face recognition privacy concerns, 35% of participants were happy for the Government to store their face information and 31% were happy for Google to store this information. To explain this result further the interviewees suggested that their face information was already out in the public domain and therefore they didn't have any concerns with it remaining that way.

> *"I'd be ok with that. My picture is on my driver's license so. Actually you know I think I'd be happy for Google to have that information too."*

> *"My face is everywhere. There's nothing private about my face."*

Of the participants that were not happy with either the Government or Google storing their face information, one interviewee expressed an interesting point in relation to the capturing of this data:

> *"I'd be afraid with face and fingerprint that someone would be compiling my data and information behind my back. Like taking pictures of me and taking my fingerprints off stuff I own and collecting all this data. At least with an iris scan, they wouldn't be able to do that. I'd have to use this scanner to give in the information. I couldn't give that information away by accident."*

This group of interviewees were then asked if they had given photographs to the Government at any stage in their lives and asked if they were happy in doing this. All interviewees indicated that they had supplied the Government with this information.

Many suggested that they had done this without thinking it through. Others felt it was acceptable to provide a hard copy photograph as they were under the impression that these photos remained in paper form and were never digitalised.

> *"I know they have my passport but I presume they don't have it digitally captured. It's just on a piece of paper somewhere in the passport office."*

The same group were then asked if they had Facebook accounts and why they were happy providing this information on Facebook but not on Google. 80% of the interviewees had Facebook or Google+ accounts. The interviewees generally could not explain why they were comfortable interacting with Facebook this way. One interviewee stated he was more comfortable allowing Google to store this information for social reason rather than using it for authentication:

> *"I'd rather them not have that information, but I've given it to Facebook for social reasons, because I wanted to share those photos with people. Whereas Google would want to use it for authentication. So I feel that that's different. One is for social reasons and the other is for security reasons."*

Regarding retina biometric, an average of 72% participants indicated that they would not give permission to the Government or Google to store their retina biometrics. Interviewees who answered similarly indicated that they felt the retina scan was as uniquely identifiable as a person's fingerprint and therefore they did not feel secure handing over this information.

The last biometric recognition type that was considered was handwriting recognition. 36% of participants were happy for the Government to have their signature information and 26% were happy for Google to have this information. Within this group of interviewees, the general consensus was that their signature was already out in the commercial domain and so therefore was no longer a security concern:

> *"Well handwriting is not really a big deal. Sure I've been signing my life away for years. I'm sure companies all over Ireland have a sample of my handwriting."*

Of the participants that were not happy with supplying this information, the general concern was identity theft:

> *"My signature is used for a lot of things like credit cards. So I'd be concerned with sharing out that information. Like if someone got hold of that information, they could potentially take out my money and use my cheques. So I wouldn't be happy with that."*

### 7.2.3 Survey Conclusion

The results collected during the CAPTCHA usage survey and interview showed that the majority of users found CAPTCHA difficult and frustrating to use. This result indicates that a more usable and accessible alternative to CAPTCHA is needed in the public domain.

The results of the biometric usage survey and interview indicated that the majority of participants did not feel comfortable with either the Government or Google storing their biometric data. This result suggests that users may not be comfortable using an application like BioScope as their biometric information would need to be stored remotely. However, from the interviews conducted it was established that although users expressed privacy concerns with the storage of their biometric information, many of these individuals had already happily provided biometric data to public and private organisations without fully considering the potential consequences. This possibly suggests that individuals can be socially engineered into providing their biometric information when necessary and therefore user satisfaction when using an application like BioScope would not be affected. It also illustrates the importance of user's trust when storing biometric information and highlights a need for a robust secure biometric storage solution.

## 7.3 Error Testing

The failure rates for each task conducted were recorded during the user testing cycle. These results are illustrated in Figure 56. During the reCAPTCHA testing a failure was recorded if the user did not successfully pass each reCAPTCHA test. A failure was

recorded during the BioScope testing if a bug was uncovered with the user interface and its navigation or if a user was unable to capture and confirm their biometric data during the biometric recognition tasks. For example during the handwriting task, a failure was recorded if the user did not correctly produce and confirm their signature. A failure was recorded during the face recognition task if the system was unable to recognise a user's face. For the voice recognition task a failure was recorded if a user did not correctly read aloud and record the five words that appeared on the screen during the test.
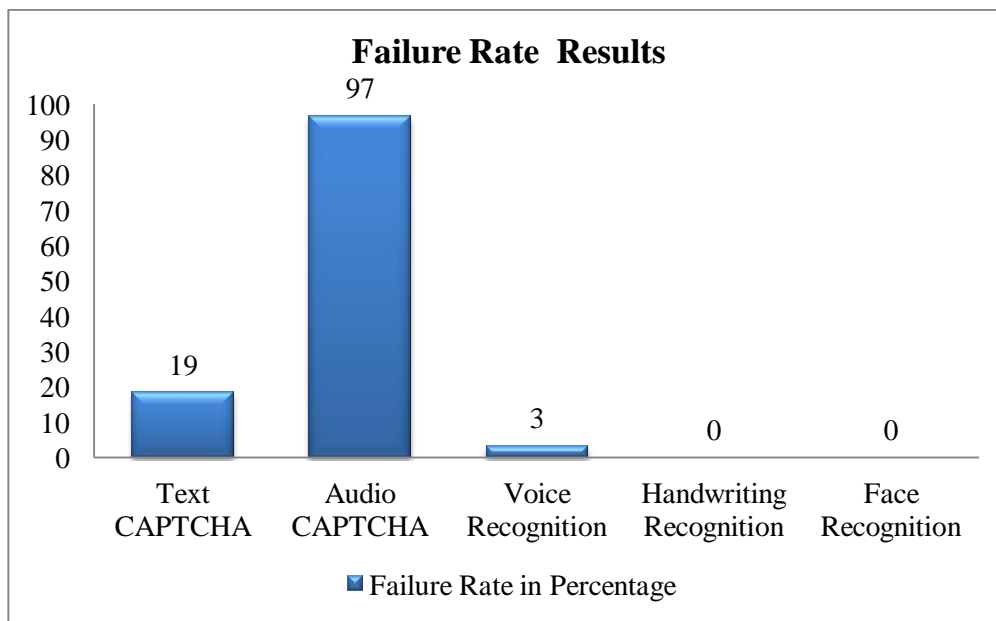


**Figure 56: Failure Rate Results**

Figure 56 shows that the text based reCAPTCHA had a failure rate of 19%. Tester F, who is dyslexic, failed 2 out of the 3 tests assigned to him. These results also illustrate the high failure rate of the audio based reCAPTCHA (97%). In contrast BioScope's voice recognition task yielded a failure rate of just 3%. Both the handwriting and face recognition testing had a 0% failure rate.

### 7.3.1 Analysis

During the testing only one user was able to complete one of the audio based reCAPTCHA test successfully. Tester J, who is blind and who would be very experienced with this using this type of CAPTCHA, was unable to pass any of the audio tests. The dyslexic tester, Tester F, listened to the audio test each time, but refused to enter anything into the text field provided as he was unsure how to spell

some of the words that he had heard. In general spelling was a concern for many of the participants. 3 participants in total made spelling mistakes when attempting to spell the words "Librarian", "February" and "Volunteer".

reCAPTCHA have previously published that the human pass rate of their system is 90%. However from the testing in the experiment this has been shown to be inaccurate. Although reCAPTCHA have not published what type of testing they conducted to achieve this figure, it is clear that a wide range of testers with varying skills and abilities were not used.

The only failure while testing the BioScope user interface was recorded while completing the voice recognition task. This failure occurred during the first testing cycle of the BioScope application. The tester recorded and confirmed their voice biometric data, however, the user had only recorded themselves saying the one out of the five words. This issue did not reoccur during the rest of the BioScope testing cycle.

These results showed that the BioScope user interface had a significantly lower error rate than the text and audio based reCAPTCHA system. However, without a server validation back-end solution for the BioScope user interface these error rate comparison results remains inconclusive. To gain a true representation of how error prone an application like BioScope would be, a full end to end solution would need to be implemented.

## 7.4 Learnability and Memorability Testing

The learnability and memorability was measured by how long each task took to complete with every attempt. The time results recorded during this user testing are illustrated in Figure 57.
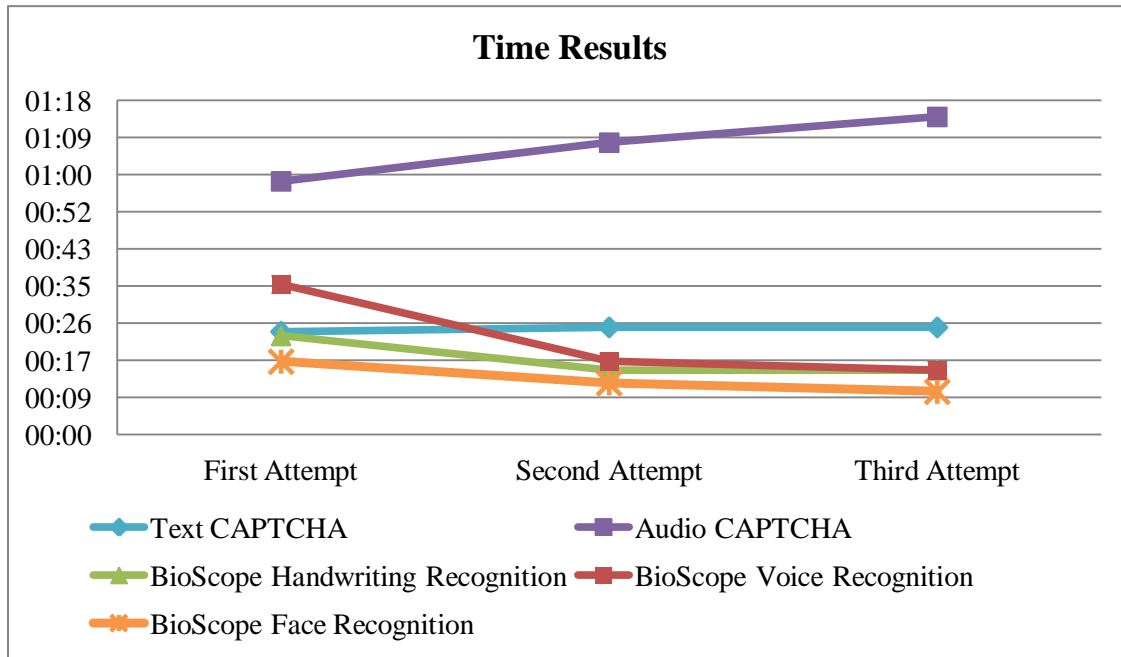
**Figure 57: Time Results**

Regarding the text based reCAPTCHA, the average time recorded during the tester's first attempt was 24 seconds. An average 25 seconds was recorded during their next attempt and their final attempt took an average of 25 seconds. The audio reCAPTCHA testing results showed that users took an average of 59 seconds, 1 minute 8 seconds and 1 minute 14 seconds for user's first, second and third attempt respectively.

BioScope's handwriting recognition task took users an average of 23 seconds during their first attempt, 15 seconds during their second attempt and 15 seconds for their last attempt. The first attempt that users conducted with the voice recognition task took an average of 35 seconds. Their second and third attempt for this task took 17 seconds and 15 seconds respectively. The final testing task involved testing BioScope's face recognition task. 17 seconds, 12 seconds and 10 seconds were the average times recorded during each user's first, second and third attempt respectively.

## 7.4.1 Analysis

The time patterns collected for both the text based and audio based reCAPTCHA systems showed that the experience gained from using these systems did not improve how effectively and efficiently a user could interact with the application. Interestingly, the more experience gained the longer each user took to complete each text based and

audio based reCAPTCHA tests. This indicates the reCAPTCHA user interface is not learnable or memorable.

In contrast users were able to improve their times when conducting each biometric recognition task; handwriting recognition, voice recognition and face recognition. This shows that, unlike the reCAPTCHA user interface, users could learn and remember how to use the BioScope application. This implies that the BioScope user interface is both learnable and memorable.

## 7.5 Efficiency Testing

Efficiency was measured by recording the time in which it took users to complete each task during their final attempt. This meant that the users had already learnt how to use the interface before the efficiency results were recorded (Nielsen 2003). The results of this testing is illustrated in Figure 58.
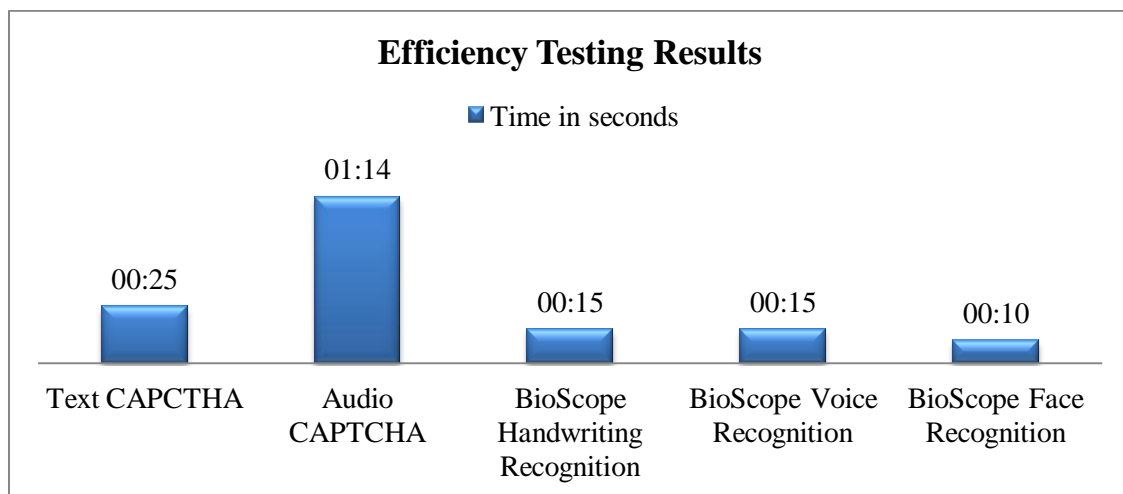


**Figure 58: Efficiency Testing Results**

In terms of efficiency, it took users an average of 25 seconds to complete their third attempt using the text based reCAPTCHA. Tester B, a novice user, completed the text based reCAPTCHA test in the shortest amount of time at 12 seconds. Tester A, also a novice user, took the longest amount of time at 43 seconds to complete the text based reCAPTCHA test.

The time results recorded during the audio based reCAPTCHA testing show that on average, it took participants 1 minute and 14 seconds to complete an audio based reCAPTCHA test during their last attempt. The longest attempt was recorded with Tester A, who took 2 minutes and 22 seconds to complete the test. Tester B conducted the test in the shortest amount of time at 21 seconds.

While testing the BioScope user interface, it took users on average 15 seconds to successfully complete a voice biometric recognition task during their last attempt. 26 seconds was the longest recorded test time by Tester A, a computer novice. Tester D (a computer expert) completed this task in the shortest amount of time in 10 seconds.

The handwriting recognition test recorded an average completion time of 15 seconds during tester's final attempt. Tester A, a computer novice, completed this test in the longest recorded time at 26 seconds. The fastest recorded time was produced by Tester E, a non native English speaker, who took 11 seconds to complete this test.
The final task involved testing BioScope's face recognition user interface. On average, it took users 10 seconds to complete their third attempt. The longest time recorded was with Tester A, a computer novice, who took 19 seconds to complete the task. Tester H, who had a mobility impairment caused by a broken elbow in his non-dominant arm, produced the fastest time in 7 seconds.

### 7.5.1  Analysis

Taken these results into account, it was established that tasks could be completed in a faster time using the BioScope application compared to both the text based reCAPTCHA and the audio based reCAPTCHA. From this, it was concluded that the BioScope user interface was more efficient than the reCAPTCHA's user interface.

## 7.6  User Satisfaction Testing

User satisfaction qualitative data was captured using the SUMI questionnaire. These results were broken into the six characteristic of user satisfaction: Efficiency, Affect, Helpfulness, Control, Learnability and Global Usability (Kirakowski et al. 1998). Each user conducted two SUMI questionnaires; the first relating to their experience with the

reCAPTCHA application and the second relating to the BioScope application. The results from this questionnaire are shown in Figure 59.



**User Satisfaction Results**

| | Efficiency | Affect | Helpfulness | Control | Learnability | Global Usability |
|---|---|---|---|---|---|---|
| CAPTCHA | 32.6 | 28.2 | 32.4 | 39.1 | 38.2 | 32.5 |
| BioScope | 64.8 | 65.2 | 61 | 54.5 | 62.7 | 63.7 |
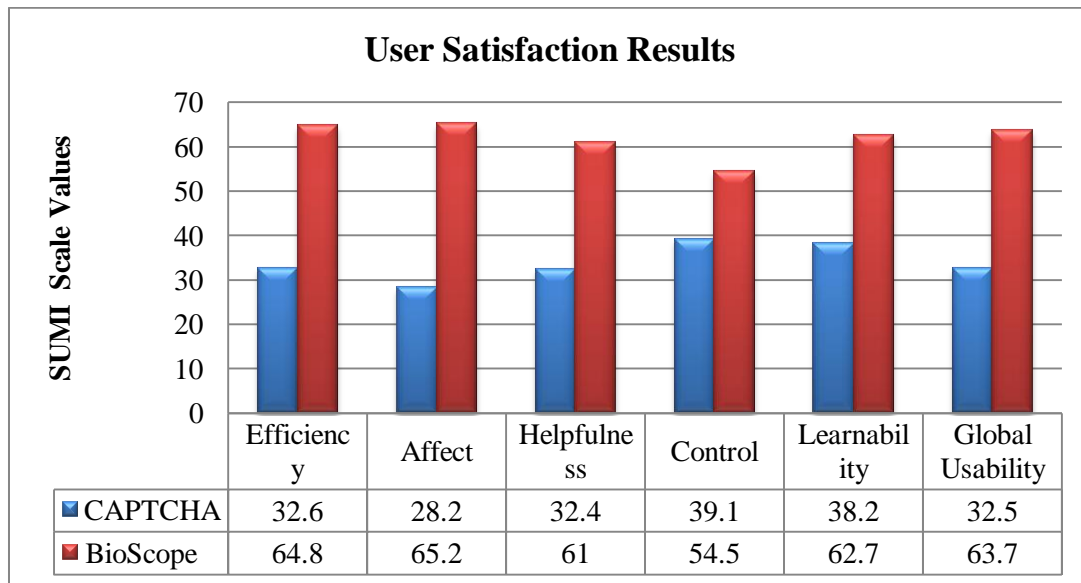
**Figure 59: User Satisfaction Results**

The reCAPTCHA system's overall user satisfaction score was 32.5 out of 100. The highest score achieved by the reCAPTCHA application was 39.1 under the Control characteristic. The lowest score of 28.2 was recorded for the Affect rating. The overall global SUMI score for the BioScope system was 63.7. The lowest score achieve by the BioScope application was 54.5 under the Control rating. The highest result of 65.2 was recorded for the Affect characteristic.

7.6.1   Analysis

90% of all users indicated in the questionnaire that using the reCAPTCHA application was frustrating. 72% agreed that using the same application was awkward. In contrast users did not find the BioScope application frustrating or awkward to use. 90% of users indicated that it was clear the needs of users had been considered when implementing the BioScope application.

All users were in agreement when asked about what improvements could be made to the reCAPTCHA application. Users felt that the words were difficult to read and the audio reCAPTCHA was difficult to understand.

*"Both the text and audio tests need to be improved. It is very hard to use both".*

*"The words are difficult to see and more instructions need to be provided with the sound test as I'm not sure how to pass it".*

The same questions were asked to users regarding what improvements could be made to the BioScope application. Generally user did not feel anything needed to be improved with the following exceptions:

*"I'd like to see other options for blind users. The voice recognition works well but might be difficult to use in a noisy environment."*

*"Maybe think of migrating this to be used on an iPhone so that even more people can use it".*

All results collected using the SUMI questionnaire show that BioScope application achieved a significantly higher user satisfaction rating than the reCAPTCHA application.

## 7.7 Analysis of Design Methodology

The results collected during the user testing show that using the inclusive design methodologies like the *Principles of Universal Design* and *Apple's User Experience Guidelines* promotes usable and accessible user interfaces. The BioScope application achieved higher ratings than the reCAPTCHA system in all 5 usable accessibility measurements; efficiency, learnability, memorability, failure rates and user satisfaction. However, these high ratings can also be contributed to the task analysis design choices.

During the task analysis the ICF framework was used to indicate what combination of biometric options should be available to a user to ensure accessibility. The ICF indicated that face recognition would be inaccessible to user with motor and visual disabilities. While this indication was correct for users with visual impairments, the testing showed that users with arm and dexterity disabilities could still capture their

face biometric data user the BioScope application. Tester H, who had a broken elbow, captured his face information by placing the iPad flat on a desk in front of him, position his face over the iPad by leaning over the desk and successfully captured a picture of his face. The ICF also indicated that a blind user would only be able to successfully complete the voice recognition task. The results from the user testing showed that this assumption was correct. The handwriting recognition task has deemed to be inaccessible for user with arm and dexterity disabilities. The testing results did not show this, however it is possible that more testing of this nature would be required with a wider range of users with motor disabilities to finalise this assumption.

## 7.8 Analysis of Testing Methodology

The usable accessibility testing methodology used during the experiment revealed that reCAPTCHA's claim of a human success rate of 90% was incorrect and inaccurate. This testing methodology showed that the success of a user interface cannot be determined using one single measurement. There are many factors that need to be met to allow an application to be usable and accessible. This might indicate that accessibility and usability should be measured using a tuple format, with each integer in the list correlating to each of the five usability measurements. See Section 8.5 for a further discussion on this tuple format.

## 7.9 Conclusion

This chapter compared and contrasted the results obtained from the reCAPTCHA and BioScope testing. These results were analysed in terms of the 5 usability measurements; learnability, memorability, efficiency, error rate and user satisfaction. Following this analysis, it was concluded that the BioScope application was more accessible and usable than the reCAPTCHA application and that the design and testing methodologies used assisted with achieving this result.

# 8 CONCLUSION AND FUTURE WORK

## 8.1 Introduction

The aim of this research was to establish an accessible alternative interface to CAPTCHA, called BioScope, using design and testing methodologies that promoted usability and accessibility. BioScope is an interface to a single sign-on system that captures user's biometric data in an accessible and usable manner exploiting in full the capabilities of the iPad tablet. This application included the use of the inbuilt microphone to capture human voice data, inbuilt camera to capture face information and its multi-touch screen to capture a person's handwriting. The BioScope interface stores this biometric data on the iPad with the potential to provide this information to a biometric recognition system on a remote server to identify if the user is a human being or a bot (the implementation of which was outside the scope of this work).

## 8.2 Research Definition & Research Overview

The area of interest for the research was that of accessibility, CAPTCHA and biometrics. These topics were explored in the literature review to help define BioScope's requirements.

Chapter 2 provided an overview of the area of accessibility. In the area of accessibility, there are two different definitions used to describe the term *disability* including a social model definition and a medical model definition. The medical model suggests that the reason for a person's disability is directly related to their physical or cognitive impairment. In contrast the social model suggests that a person's disability is caused by social and environmental barriers. There are many different types of disabilities including visual, physical and cognitive disabilities. People with these disabilities may find it difficult to see, to move or to read and write. These difficulties can be experienced in the built environment or in domain of information technology. To help resolve these issues assistive technologies can be used, including a screen reader that reads aloud the information on a computer screen for blind users, and switch access devices which enable individuals with motor disabilities to interact with a computer user interface. Ensuring that assistive technologies are compatible with computer user

interfaces presents some unique challenges for interface designers, developers and testers. There are many usability and accessibility guidelines, principles and tools that aim to guide designers and developers to create accessible computer systems. For example the *Web Content Accessibility Guidelines 2.0* encourages web developers to produce accessible web content and the *Principles of Universal Design* support designers in implementing universally inclusive products.

Chapter 3 discussed the different types of CAPTCHA available to Internet users. CAPTCHA is an automated system that is designed to tell humans and computers apart using visual or audio tests that are designed so that humans can pass them easily, but that bots cannot. Overall CAPTCHA systems are used more than 200 million times every single day (Google 2012) and claim a human pass rate of 90% (L. Von Ahn et al. 2008). However, CAPTCHA poses many usability and accessibility issues for people with disabilities suggesting that the published human pass rate figure is not accurate and does not consider people with varying disabilities.

The use of biometrics as an alternative to CAPTCHA was suggested by W3C (W3C 2005). Chapter 4 explored this area of biometrics. Biometrics can be broken into two categories; physiological biometrics and behavioural biometrics. Physiological biometrics is collected by measuring parts of a human body, for example fingerprint and retina biometrics. Behavioural biometrics is collected by measuring a person's actions, for example voice and handwriting biometrics. Physiological biometrics are considered more secure that behavioural biometrics, however, both types of biometric are used in computer systems around the world, ranging from face recognition used at airport's passport control stations and handwriting used during bank transactions.

Using this information gained from the literature review, a design and testing methodology was outlined in the context of BioScope's design and evaluation process in Chapter 5. Using the *Star Lifecycle Model*, a user centric design methodology, user and system requirements were identified and evaluated at each phase using interviews, prototypes and accessibility/usability guidelines and principles. For use in BioScope, the International Classification of Functioning (ICF) identified what combinations of physiological and behavioural biometric recognition methods were accessible and usable for a diverse user base. The *Principles of Universal Design* and *Apple's User*

*Experience Guidelines* assisted with the development of BioScope's accessible user interface. A usable accessibility testing methodology was devised to test both reCAPTCHA's and BioScope's user interface. Using *usable accessibility* measurements, the reCAPTCHA and BioScope systems were compared and contrasted with the aim of determining if BioScope was a viable alternative to CAPTCHA.

## 8.3 Contributions to the Body of Knowledge

In the literature, CAPTCHA systems claim to have a human pass rate of 90% (L. Von Ahn et al. 2008). In all the research, the testing procedure that yielded this 90% success rate was not outlined. It remains unknown how many users were used during this testing and if this user testing group had a diverse set of abilities and disabilities. This previous testing identified a pass result when a user successfully passed a text based reCAPTCHA test. However, there are other factors that need to be considered when trying to establish if a system is usable, like task efficiency and user satisfaction. In order to test reCAPTCHA for this project, a user testing methodology was used to establish if reCAPTCHA's claim of a human pass rate of 90% was accurate. For this, a testing strategy was outlined using usability and accessibility measurements.

Usability implies that a specified user can use a product with ease. The ease of use can be measured in terms of how accurately a task can be completed by a user, the time it takes a user to complete a task and how satisfied the user is with the overall experience of using the product. These usability factors are further explored by Nielsen's five usability measurements: learnability, efficiency, failure rate, memorability and user satisfaction.

Accessibility implies that a diverse group of users with varying disabilities can use a product with ease. The measurements for this ease of use are less clear in the realm of accessibility. The W3C published the *Web Content Accessibility Guidelines 2.0* (WCAG 2.0) that outline techniques that web developers and designers can avail of in order to create accessible web content. However, there are two factors that these guidelines do not consider. Firstly these guidelines are designed for web content and not for other software or application development. While some of the guidelines can be considered, many of the guidelines are not relevant when designing computer software.

Secondly these guidelines focus on how a user interacts with a website, but they do not consider the user's interaction experience and how this experience is measured.

For the experiment, the pre-existing usability measurements (Nielsen's 5 Usability Characteristics) were combined with the philosophy of accessibility, creating a usable accessibility testing methodology. This measured the interaction experience of a wide range of users, with varying disabilities. It was this testing methodology that was used during the experiment to determine if the BioScope user interface was more usable and accessible than the reCAPTCHA system.

## 8.4 Experimentation, Evaluation and Limitation

The aim of the experiment was to determine if BioScope, a biometric alternative interface to CAPTCHA, was more accessible and usable than reCAPTCHA by using a usable accessibility testing methodology.

Ten users with varying skills, abilities and disabilities in total tested both the reCAPTCHA system and the BioScope system. All data was recorded in terms of efficiency, learnability, memorability, failure rates and user satisfaction. Success in these five areas would determine if the relevant system was accessible and usable.

To test for efficiency users were timed while completing the relevant tasks with both reCAPTCHA and BioScope. Users took an average of 25 seconds to complete a text based CAPTCHA and 1 minute 14 seconds to complete an audio based CAPTCHA. In contrast users took an average of 13 seconds to complete a BioScope task thus showing that BioScope was more efficient than reCAPTCHA.

Testers repeated each system task a total of three times. When conducting the testing with the reCAPTCHA user interface, user did not increase the time in which it took them to complete the task with each attempt, whereas the opposite was observed with the BioScope testing. This showed that BioScope's user interface was more learnable than the reCAPTCHA system.

When considering the human pass rate of these systems, the testing showed that the text based reCAPTCHA system had a human pass rate of 81% and the audio based reCAPTCHA system had a human pass rate of only 3%. These results indicate that reCAPTCHA's human pass rate of 90%, previously outlined by Von Ahn et al, is not accurate. BioScope achieved a human pass rate of 97% during test. However as the BioScope application was not a full end to end solution it was unable to determine whether the biometric information supplied by a user was correct. This means that these results did not truly reflect the human pass rate for BioScope. Therefore the result of the error tolerance testing remains inconclusive.

The final element of testing focused on user's satisfaction. The user satisfaction testing showed that reCAPTCHA achieved a low user satisfaction rating of 32.5%. In contrast BioScope achieved a user satisfaction level of 63.7%.

Overall these testing results showed that the BioScope user interface was more usable and accessible than the reCAPTCHA system with two limitations:

Firstly, it was suggested in the literature the use of biometrics may cause some privacy concerns with the people that use these biometric systems. This was an area explored during the experiment using a survey and interview process. In total 70 people were surveyed and 10 individuals were interviewed. Participants were asked if they would be comfortable with supplying biometric data, like face information, voice information and fingerprint information, to a private organisation and a public organisation. While there were some differences in comfort levels with the supply of each biometric data type, overall the majority of participants were not comfortable with supplying this type of information. The user satisfaction testing showed that the BioScope system received a user satisfaction rating of 63.7%, however it is unclear if this rating was affected by some of these biometric privacy concerns. If testers were aware of all the privacy issues they may not have been comfortable with using the BioScope application and therefore given a lower user satisfaction rating.

Secondly the BioScope system testing was limited to testing the user interface itself. This included navigating through the system, entering in textual details and capturing biometric data. No biometric information was passed to or validated by a remote

server. Taking this into consideration, a fully operational BioScope application, including server functionality, may increase the response times and failure rates.

## 8.5 Future Work & Research

Taking the limitations of the experiment into account there are three main areas that could be further explored with the aim of producing an accessible biometric alternative to CAPTCHA:

The BioScope application did not implement any remote server side biometric validation or storage. This is an area where extensive research could be carried out in terms of generating the captured data from the iPad into a biometric template. This research would include assessing how accurate and valid the information captured by an iPad tablet is. For storing this information, security techniques and policies would need to be understood and implemented to ensure that people's biometric information was secure.

The second area of research could attempt to further understand people's privacy concerns in terms of biometric usage. The survey conducted in this project indicated that people were not comfortable with supplying biometric information relating to their face, voice, handwriting, retina and fingerprint. However the interview results suggested that although people had these concerns, they had still provided their biometric information to various public and private organisations with little issue. It is this dynamic between user's initial concerns and the social engineering of these concerns that could be investigated more.

Lastly, further research and investigation could be carried out in the area of usability and accessibility measurements. The results collected from the experiment show that using one metric (the human pass rate) does not accurate indicate how accessible or usable a user interface is. There are many factors that need to be considered when assessing a user interface including efficiency, failure rates, learnability, memorability and user satisfaction. Potentially these five factors could be represented in a tuple format, with each integer in the list correlating to each of the usability factor.

## *8.6 Conclusion*

The current implementation of CAPTCHA, whether visual or audio, presents users with many challenges in terms of accessibility and usability. Using a usable accessibility testing methodology, an alternative interface to CAPTCHA was designed and developed. This system, called BioScope, captures user's biometric data in an accessible and usable manner availing of the various capabilities of the iPad tablet, including camera, microphone and gesture recognition.

Using a testing methodology, that combined the philosophies of usability and accessibility, it was shown that the BioScope user interface was more accessible and usable than the reCAPTCHA system.

With further investigation in the area of biometric recognition and security, BioScope's full potential to replace the existing CAPTCHA systems can be one day be realised.

# 9    REFERENCES

Adeyinka, O., 2008. Internet Attack Methods and Internet Security Technology. In *Proceedings of the 2008 Second Asia International Conference on Modelling & Simulation (AMS)*. AMS '08. Washington, DC, USA: IEEE Computer Society, pp. 77–82. Available at: http://dx.doi.org/10.1109/AMS.2008.68 [Accessed June 23, 2012].

Adini, Y., Moses, Y. & Ullman, S., 1997. Face recognition: The problem of compensating for changes in illumination direction. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 19(7), pp.721–732.

Von Ahn, L., 2009. Human computation. In *Design Automation Conference, 2009. DAC'09. 46th ACM/IEEE*. pp. 418–419. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5227025 [Accessed June 23, 2012].

Von Ahn, L. et al., 2008. recaptcha: Human-based character recognition via web security measures. *Science*, 321(5895), pp.1465–1468.

von Ahn, L., Blum, M. & Langford, J., 2002. Telling humans and computers apart automatically or how lazy cryptographers do AI. *Computer Science Department*, p.149.

Von Ahn, L. & Dabbish, L., 2004. Labeling images with a computer game. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. pp. 319–326. Available at: http://dl.acm.org/citation.cfm?id=985733 [Accessed June 25, 2012].

Ahn, L.V. et al., 2003. CAPTCHA: Using hard AI problems for security. In *Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques*. pp. 294–311.

Ahn, Luis Von & Cathcart, W., 2009. Teaching computers to read: Google acquires reCAPTCHA | Official Google Blog. Available at: http://googleblog.blogspot.ie/2009/09/teaching-computers-to-read-google.html [Accessed June 23, 2012].

Alver, C., 2007. Voice Biometrics in Financial Services. *Journal of Financial Services Technology, The*, 1(1), p.75.

Andrews, D., Nonnecke, B. & Preece, J., 2003. Electronic survey methodology: A case study in reaching hard-to-involve Internet users. *International Journal of Human-Computer Interaction*, 16(2), pp.185–210.

Apple, 2010. iOS Human Interface Guidelines: User Experience Guidelines. Available at: https://developer.apple.com/library/ios/#documentation/UserExperience/Conceptual/MobileHIG/UEBestPractices/UEBestPractices.html#//apple_ref/doc/uid/TP40006556-CH20-SW1 [Accessed February 19, 2012].

Apple Inc., 2012. Apple - iPad 2 - View the technical specifications for iPad 2. Available at: http://www.apple.com/ipad/ipad-2/specs.html [Accessed June 9, 2012].

Apple Inc., 2010. iOS Human Interface Guidelines: iOS UI Element Usage Guidelines. Available at: http://developer.apple.com/library/ios/#DOCUMENTATION/UserExperience/Conceptual/MobileHIG/UIElementGuidelines/UIElementGuidelines.html#//apple_ref/doc/uid/TP40006556-CH13-SW1 [Accessed June 19, 2012].

Apple Inc., 2005. United States Patent: 7800592. Available at: http://patft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=7,800,592.PN.&OS=PN/7,800,592&RS=PN/7,800,592 [Accessed April 14, 2012].

Arh, T. & Blažič, B.J., 2008. A case study of usability testing: the SUMI evaluation approach of the EducaNext portal. *WSEAS Transactions on Information Science and Applications*, 5(2), pp.175–181.

Arthritis Ireland, 2012. About Arthritis - Arthritis Ireland. Available at: http://www.arthritisireland.ie/go/about_arthritis [Accessed July 6, 2012].

Asakawa, C., 2005. What's the web like if you can't see it? In *Proceedings of the 2005 International Cross-Disciplinary Workshop on Web Accessibility (W4A)*. pp. 1–8. Available at: http://dl.acm.org/citation.cfm?id=1061813 [Accessed July 7, 2012].

Assist Ireland, 2012. Switch Access. *mc*. Available at: http://www.assistireland.ie/eng/Information/Communication/Switch_Access.html [Accessed July 7, 2012].

Assist IT, 2012. Switch Access. Available at: http://www.assist-it.org.uk/assets/content/switch_access.htm [Accessed July 15, 2012].

Atlassian, 2012. Crowd | Atlassian. Available at: http://www.atlassian.com/software/crowd/overview [Accessed July 15, 2012].

Australian Customs Service, 2012. SmartGate. *SmartGate*. Available at: http://www.customs.gov.au/smartgate/default.asp [Accessed June 22, 2012].

Bigham, J.P. & Cavender, A.C., 2009. Evaluating existing audio captchas and an interface optimized for non-visual use. In *Proceedings of the 27th international conference on Human factors in computing systems*. pp. 1829–1838.

Di Blas, N., Paolini, P. & Speroni, M., 2004. Usable accessibility" to the Web for blind users. In *Proceedings of 8th ERCIM Workshop: User Interfaces for All, Vienna*. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.110.8239&rep=rep1&type=pdf [Accessed July 10, 2012].

Blenkhorn, P. & Evans, G., 2000. Architecture and requirements for a Windows screen reader. In *Speech and Language Processing for Disabled and Elderly People (Ref. No. 2000/025), IEE Seminar on*. pp. 1–1. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=846939 [Accessed July 7, 2012].

Breaux, T.D. et al., 2008. Legal requirements, compliance and practice: an industry case study in accessibility. In *International Requirements Engineering, 2008. RE'08. 16th IEEE*. pp. 43–52. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4685651 [Accessed July 14, 2012].

Brian, G. & Taylor, H., 2001. Round Table-Cataract blindness-Challenges for the 21st century. *Bulletin of the World Health Organization*, 79(3), pp.249–256.

Brisenden, S., 1986. Independent living and the medical model of disability. *Disability, Handicap & Society*, 1(2), pp.173–178.

Bruce, V. & Young, A., 1986. Understanding face recognition. *British journal of psychology*, 77(3), pp.305–327.

Brunelli, R. & Poggio, T., 1993. Face recognition: Features versus templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 15(10), pp.1042–1052.

Büchel, C., 1998. Functional neuroimaging studies of Braille reading: cross-modal reorganization and its implications. *Brain*, 121(7), pp.1193–1194.

C.L.Gupta Eye Institute, 2009. C.L.Gupta Eye Institute - Vision For All. Available at: http://www.clgei.org/glaucoma.htm [Accessed July 15, 2012].

CAD, P., 2001. International classification of functioning, disability and health (ICF). Available at: http://publications.cpha.ca/products/2-1152088 [Accessed July 7, 2012].

Calder, A.J. & Young, A.W., 2005. Understanding the recognition of facial identity and facial expression. *Nature Reviews Neuroscience*, 6(8), pp.641–651.

Cantor Access Inc., 2012. Cantor Access - Consulting - Seminars - AODA Training. Available at: http://www.cantoraccess.com/consulting/course1_disability.html [Accessed July 15, 2012].

Cense, B. et al., 2002. Invivo depth-resolved birefringence measurements of the human retinal nerve fiber layer by polarization-sensitive optical coherence tomography. *Optics Letters*, 27(18), pp.1610–1612.

Center for Universal Design, 2008. The Center for Universal Design - About UD. Available at: http://www.ncsu.edu/www/ncsu/design/sod5/cud/about_ud/about_ud.htm [Accessed July 7, 2012].

Central Statistics Office, 2007. *Volume 11 Disability, Carers and Voluntary Activites*, Available at: http://www.cso.ie/en/media/csoie/census/census2006results/volume11/Volume 11_2006.pdf.

Chandavale, A.A. & Sapkal, A.M., 2011. Reduced Process Thinning Algorithm for CAPTCHA Strength Measurement.

Chellapilla, K. et al., 2005. Designing human friendly human interaction proofs (HIPs). In *Proceedings of the SIGCHI conference on Human factors in computing systems*. pp. 711–720. Available at: http://dl.acm.org/citation.cfm?id=1055070 [Accessed July 1, 2012].

Cheng, Y. & Larin, K.V., 2007. In vivo two-and three-dimensional imaging of artificial and real fingerprints with optical coherence tomography. *Photonics Technology Letters, IEEE*, 19(20), pp.1634–1636.

Cieza, A. et al., 2002. Linking health-status measurements to the international classification of functioning, disability and health. *Journal of Rehabilitation Medicine*, 34(5), pp.205–210.

Cole, S., 2004. History of fingerprint pattern recognition. *Automatic fingerprint recognition systems*, pp.1–25.

Coleman, R. et al., 2007. Design for Inclusivity. *Gower Publishing Ltd, England Kujala S (2008) Effective User Involvement in Product Development by Improving the Analysis of User Needs. Behaviour & Information Technology*, 27, pp.457–473.

Coleman, R. et al., 2011. What is inclusive design? Available at: http://www.inclusivedesigntoolkit.com/betterdesign2/whatis/whatis.html [Accessed July 8, 2012].

Cooke, A., 2004. *A History of Accessibility at IBM*, AFB Press, American Foundation for the Blind.

Costabile, M.F., 2001. Usability in the software life cycle. *Handbook of software engineering and knowledge engineering*, 1, pp.179–192.

Crow, L., 2010. Including all of our lives. *Equality, participation and inclusion 1: diverse perspectives*, p.124.

DAI, 2012. General Information about Dyslexia «☐Dyslexia Association of Ireland. Available at: http://www.dyslexia.ie/information/general-information-about-dyslexia/ [Accessed July 6, 2012].

Daugman, J., 2004. How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1), pp.21–30.

Davies, T.C. et al., 2010. Enabling self-directed computer use for individuals with cerebral palsy: a systematic review of assistive devices and technologies. *Developmental Medicine & Child Neurology*, 52(6), pp.510–516.

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

Doidge, 2012. Brain Plasticity | Cellfield Canada. Available at: http://cellfield.ca/how-cellfield-works/brain-plasticity/ [Accessed July 8, 2012].

Duara, R. et al., 1991. Neuroanatomic differences between dyslexic and normal readers on magnetic resonance imaging scans. *Archives of Neurology*, 48(4), p.410.

Duffy, T.J., 2011. CAPTCHA Advertising Coming Soon To A Website Near You. *Techi.com*. Available at: http://www.techi.com/2010/04/captcha-advertising-coming-soon-to-a-website-near-you/ [Accessed July 15, 2012].

Dugelay, J.L. et al., 1993. Recent advances in biometric person authentication. In *Acoustics, Speech, and Signal Processing, 1993. ICASSP-93., 1993 IEEE International Conference on*. p. IV–IV. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1004810 [Accessed June 22, 2012].

Elson, J. et al., 2007. Asirra: a CAPTCHA that exploits interest-aligned manual image categorization. *CCS*, 7, pp.366–374.

EmpowHer, 2012. Women's Health & Wellness Social Community - Health Info & Resources. Available at: http://www.empowher.com/ [Accessed July 15, 2012].

Fänge, A. & Iwarsson, S., 2003. Accessibility and usability in housing: Construct validity and implications for research and practice. *Disability & Rehabilitation*, 25(23), pp.1316–1325.

Faulkner, L., 2003. Beyond the five-user assumption: Benefits of increased sample sizes in usability testing. *Behavior Research Methods*, 35(3), pp.379–383.

Faundez-Zanuy, M., 2006. Biometric security technology. *Aerospace and Electronic Systems Magazine, IEEE*, 21(6), pp.15–26.

Faundez-Zanuy, M., 2005. Signature recognition state-of-the-art. *Aerospace and Electronic Systems Magazine, IEEE*, 20(7), pp.28 – 32.

Golle, P., 2008. Machine learning attacks against the Asirra CAPTCHA. In *Proceedings of the 15th ACM conference on Computer and communications security*. pp. 535–542. Available at: http://dl.acm.org/citation.cfm?id=1455838 [Accessed June 23, 2012].

Goodin, A., 2012. How a trio of hackers brought Google's reCAPTCHA to its knees | Ars Technica. Available at: http://arstechnica.com/security/2012/05/google-recaptcha-brought-to-its-knees/ [Accessed June 23, 2012].

Google, 2012. reCAPTCHA Security. Available at: http://www.google.com/recaptcha/security [Accessed June 23, 2012].

GreatBuildings, 2012. Robson Square - Arthur C. Erickson - Great Buildings Architecture. Available at: http://www.greatbuildings.com/buildings/Robson_Square.html [Accessed July 8, 2012].

Groosoft, 2012. Blueprint for iPad on the iTunes App Store. Available at: http://itunes.apple.com/us/app/blueprint/id405203705?mt=8 [Accessed February 22, 2012].

Groß, T., 2003. Security analysis of the SAML single sign-on browser/artifact profile. In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*. pp. 298–307. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1254334 [Accessed July 14, 2012].

Guru, D.S. et al., 2011. An Approach for Hand Vein Representation and Indexing. *International Journal of Digital Crime and Forensics (IJDCF)*, 3(2), pp.1–15.

Halle, M. & Stevens, K., 1962. Speech recognition: A model and a program for research. *Information Theory, IRE Transactions on*, 8(2), pp.155 –159.

Haxby, J.V., Hoffman, E.A. & Gobbini, M.I., 2000. The distributed human neural system for face perception. *Trends in cognitive sciences*, 4(6), pp.223–233.

Hernandez-Castro, C.J., Ribagorda, A. & Hernandez-Castro, J.C., 2010. ON THE STRENGTH OF EGGLUE. Available at: http://www.azlaha.com/SECRYPT2011EgglueTextCAPTCHA.pdf [Accessed June 23, 2012].

Hix, D. & Hartson, H.R., 1993. *Developing user interfaces: ensuring usability through product & process*, John Wiley & Sons.

Hong, L. & Jain, A., 1998. Integrating faces and fingerprints for personal identification. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 20(12), pp.1295–1307.

Hou, W., Ye, X. & Wang, K., 2004. A survey of off-line signature verification. In *Intelligent Mechatronics and Automation, 2004. Proceedings. 2004 International Conference on*. pp. 536 – 541.

HSE, 2012. Causes of dyslexia. Available at: http://www.hse.ie/eng/services/flu/A-Z/D/Dyslexia/Causes-of-dyslexia.html [Accessed July 6, 2012].

Huang, X. & Lee, K.F., 1993. On speaker-independent, speaker-dependent, and speaker-adaptive speech recognition. *Speech and Audio Processing, IEEE Transactions on*, 1(2), pp.150–157.

ISO, 2010. ISO 9241-210:2010 - Ergonomics of human-system interaction -- Part 210: Human-centred design for interactive systems. Available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=52075 [Accessed July 8, 2012].

Jaeger, P.T., 2002. Section 508 goes to the library: Complying with federal legal standards to produce accessible electronic and information technology in libraries. *Information Technology and Disabilities*, 8(2). Available at: http://www.freepatentsonline.com/article/Information-Technology-Disabilities/207644357.html [Accessed July 14, 2012].

Jain, A., Bolle, R. & Pankanti, S., 2002. Introduction to biometrics. *Biometrics*, pp.1–41.

Jain, A. K., Nandakumar, K. & Nagar, A., 2008. Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008, p.113.

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

Jain, Anil K., Griess, F.D. & Connell, S.D., 2002. On-line signature verification. *Pattern Recognition*, 35(12), pp.2963–2972.

Jette, A.M. & Branch, L.G., 1981. The Framingham disability study: II. Physical disability among the aging. *American Journal of Public Health*, 71(11), pp.1211–1216.

Judy, J., 2005. Usability assessment of academic digital libraries: Effectiveness, efficiency, satisfaction, and learnability. *Assessment*, 55, pp.96–121.

Juels, A., Molnar, D. & Wagner, D., 2005. Security and privacy issues in e-passports. In *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*. pp. 74–88. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1607561 [Accessed June 22, 2012].

Kang, H. et al., 2003. A study on performance evaluation of fingerprint sensors. In *Audio-and Video-Based Biometric Person Authentication*. pp. 1055–1055. Available at: http://www.springerlink.com/index/0n9xyeh420d733bl.pdf [Accessed June 22, 2012].

Kelly, B. et al., 2005. Forcing standardization or accommodating diversity?: a framework for applying the WCAG in the real world. In *Proceedings of the 2005 International Cross-Disciplinary Workshop on Web Accessibility (W4A)*. pp. 46–54. Available at: http://dl.acm.org/citation.cfm?id=1061820 [Accessed July 14, 2012].

Kirakowski, J., 2012. What is SUMI? Available at: http://sumi.ucc.ie/whatis.html [Accessed July 8, 2012].

Kirakowski, J., Claridge, N. & Whitehand, R., 1998. Human centered measures of success in web site design. In *Proceedings of the Fourth Conference on Human Factors & the Web*. Available at: http://research.microsoft.com/en-us/um/people/marycz/hfweb98/kirakowski/ [Accessed June 24, 2012].

Kittleson, M.J., 1997. Determining effective follow-up of e-mail surveys. *American Journal of Health Behavior*, 21(3), pp.193–196.

Krawczyk, S. & Jain, A., 2005. Securing electronic medical records using biometric authentication. In *Audio-and Video-Based Biometric Person Authentication*. pp. 435–444. Available at: http://www.springerlink.com/index/7m1qtdjuxjw7h9vb.pdf [Accessed June 22, 2012].

Lang, T., 2003. Comparing website accessibility evaluation methods and learnings from usability evaluation methods. *Peak Usability*, (December).

Lévesque, V. et al., 2005. Display of virtual braille dots by lateral skin deformation: feasibility study. *ACM Transactions on Applied Perception (TAP)*, 2(2), pp.132–149.

Lim, S. et al., 2001. Efficient iris recognition through improvement of feature vector and classifier. *ETRI journal*, 23(2), pp.61–70.

Mariotti, S.P., Pascolini, D. & Rose-Nussbaumer, J., 2009. Trachoma: global magnitude of a preventable cause of blindness. *British Journal of Ophthalmology*, 93(5), pp.563–568.

Matsumoto, T. et al., 2002. Impact of artificial gummy fingers on fingerprint systems. In *Proceedings of SPIE*. pp. 275–289. Available at: http://cryptome.info/0001/gummy/gummy.htm [Accessed June 22, 2012].

McLawhorn, L., 2001. Leveling the accessibility playing field: Section 508 of the Rehabilitation Act. *NCJL & Tech.*, 3, p.63.

Metwest Eye Centre, 2012. Metwest Eye Centre - Eye Conditions - About Cataracts. Available at: http://www.metwesteyecentre.com.au/eye-conditions-details.php?conditions_id=1 [Accessed July 15, 2012].

Miller, G.A., 1956. The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological review*, 63(2), p.81.

Mori, G. & Malik, J., 2003a. Breaking a Visual CAPTCHA. Available at: http://www.cs.sfu.ca/~mori/research/gimpy/ [Accessed July 15, 2012].

Mori, G. & Malik, J., 2003b. Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA. In *Computer Vision and Pattern Recognition, 2003. Proceedings. 2003 IEEE Computer Society Conference on*. p. I–134. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1211347 [Accessed June 23, 2012].

Moy, G. et al., 2004. Distortion estimation techniques in solving visual CAPTCHAs. In *Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference on*. p. II–23. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1315140 [Accessed June 23, 2012].

MS Ireland, 2011. What is ms?□:: MS Ireland. Available at: http://www.ms-society.ie/pages/what-is-ms [Accessed July 6, 2012].

Mulvany, J., 2000. Disability, impairment or illness? The relevance of the social model of disability to the study of mental disorder. *Sociology of Health & Illness*, 22(5), pp.582–601.

NALA, 1997. The main research - OECD International Adult Literacy Survey | NALA. Available at: http://www.nala.ie/main-research-oecd-international-adult-literacy-survey [Accessed July 14, 2012].

NCBI, 2012a. Cataracts. Available at: http://www.ncbi.ie/information-for/eye-health-and-eye-care/eye-conditions/cataracts [Accessed July 6, 2012].

NCBI, 2012b. Most Common Causes of Sight Loss. *Most common causes of sight loss*. Available at: http://www.ncbi.ie/information-for/friends-and-relatives/most-common-causes-of-sight-loss [Accessed July 6, 2012].

NDA, 2012. What is Universal Design. Available at: http://www.universaldesign.ie/exploreampdiscover [Accessed October 29, 2011].

Nelson, W., Turin, W. & Hastie, T., 1994. Statistical methods for on-line signature verification. *IJPRAI*, 8(3), pp.749–770.

Nielsen, J., 2003. Usability 101: Introduction to usability. *Jakob Nielsen's Alertbox*, 25. Available at: http://www.hh.se/download/18.5173bcf712de11663378000958/diskussionsupp gift_F5_nielsen.pdf [Accessed June 20, 2012].

Nielsen, J., 2000. Why you only need to test with 5 users. *Test*, 19(September 23).

Norman, D.A., 2004. *Emotional design: Why we love (or hate) everyday things*, Basic Civitas Books.

O'Connor, J., 2011. *Real World User Testing: An Assessment of User Testing Methodologies in Theory and Practice*. Dublin Institute of Technology.

O'Leary, C. & Gordon, D., 2009. Universal design, education and technology. In 9th. IT & T Conference. Dublin Institute of Technology.

Paulesu, E. et al., 2001. Dyslexia: cultural diversity and biological unity. *Science*, 291(5511), p.2165.

Pentland, A., Moghaddam, B. & Starner, T., 1994. View-based and modular eigenspaces for face recognition. In *Computer Vision and Pattern Recognition, 1994. Proceedings CVPR'94., 1994 IEEE Computer Society Conference on*. pp. 84–91. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=323814 [Accessed June 24, 2012].

Perenboom, R.J.M. & Chorus, A.M.J., 2003. Measuring participation according to the International Classification of Functioning, Disability and Health (ICF). *Disability & Rehabilitation*, 25(11-12), pp.577–587.

Petrie, H. & Kheir, O., 2007. The relationship between accessibility and usability of websites. In *CHI-CONFERENCE-*. p. 397. Available at: http://www.takebay.net/data/chi07/docs/p397.pdf [Accessed July 8, 2012].

Pfitzmann, B. & Waidner, M., 2003. Analysis of liberty single-sign-on with enabled clients. *Internet Computing, IEEE*, 7(6), pp.38–44.

Pinar Saygin, A., Cicekli, I. & Akman, V., 2000. Turing Test: 50 Years Later. *Minds Mach.*, 10(4), pp.463–518.

Poynter, L., 2002. Setting the standard: Section 508 could have an impact on private sector Web sites through the Americans with Disabilities Act. *Ga. St. UL Rev.*, 19, p.1197.

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

Reid, L.G. & Snow-Weaver, A., 2008. WCAG 2.0: a web accessibility standard for the evolving web. In *Proceedings of the 2008 international cross-disciplinary conference on Web accessibility (W4A)*. pp. 109–115. Available at: http://dl.acm.org/citation.cfm?id=1368069 [Accessed July 7, 2012].

Reimer-Reiss, M., 2000. Assistive technology discontinuance. In *Technology and Persons with Disabilities Conference*.

Reynolds, D.A. & Rose, R.C., 1995. Robust text-independent speaker identification using Gaussian mixture speaker models. *Speech and Audio Processing, IEEE Transactions on*, 3(1), pp.72–83.

Sauer, G. et al., 2008. Towards a universally usable CAPTCHA. In *Proceedings of the Symposium on Accessible Privacy and Security, ACM Symposium On Usable Privacy and Security (SOUPS'08), Pittsburgh, PA, USA*. Available at: http://cups.cs.cmu.edu/soups/2008/SOAPS/sauer.pdf [Accessed June 23, 2012].

Sayeed, S., Kamel, N.S. & Besar, R., 2007. Virtual reality based dynamic signature verification using data glove. In *Intelligent and Advanced Systems, 2007. ICIAS 2007. International Conference on*. pp. 1260–1264. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4658586 [Accessed June 22, 2012].

Selwyn, N. & Robson, K., 1998. Using e-mail as a research tool. *Social research update*, 21, pp.1–4.

SFA, 2012. Barrier-Free World Vision - Braille. Available at: http://www.sterlingfrazer.com/BFW/Vision/Braille.html [Accessed July 15, 2012].

Sheehan, K.B., 2001. E-mail survey response rates: A review. *Journal of Computer-Mediated Communication*, 6(2), pp.0–0.

Shin, Dongwan, Ahn, G.-J. & Shenoy, P., 2004. Ensuring information assurance in federated identity management. In *Performance, Computing, and Communications, 2004 IEEE International Conference on*. pp. 821 – 826.

Smith, J., 2009. WebAIM: Blog - Screen Reader Survey Results. Available at: http://webaim.org/blog/screen-reader-survey-results/ [Accessed July 7, 2012].

Smith, S.D., Kelley, P.M. & Brower, A.M., 1998. Molecular approaches to the genetic analysis of specific reading disability. *Human biology*, 70(2), p.239.

SSB BART Group, 2011. Second ANPRM on Section 508 from US Access Board Due Out First Week of December | SSB BART Group. Available at: https://www.ssbbartgroup.com/blog/2011/11/17/second-anprm-on-section-508-from-us-access-board-due-out-first-week-of-december/ [Accessed July 14, 2012].

Standardization, I.-I.O. for, 2011. ISO - International Organization for Standardization. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50864 [Accessed June 22, 2012].

Stone-Gross, B. et al., 2011. The underground economy of spam: A botmaster's perspective of coordinating large-scale spam campaigns. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*. Available at: http://static.usenix.org/events/leet11/tech/full_papers/Stone-Gross.pdf [Accessed July 5, 2012].

Sullivan, T. & Matson, R., 2000. Barriers to use: usability and content accessibility on the Web's most popular sites. In *Proceedings on the 2000 conference on Universal Usability*. pp. 139–144. Available at: http://dl.acm.org/citation.cfm?id=355549 [Accessed July 7, 2012].

Symantec, 2011. *MessageLabs Intelligence Report*, Available at: http://www.symanteccloud.com/mlireport/MLI_2011_05_May_FINAL-en.pdf [Accessed July 5, 2012].

Thatcher, J., 1994. Screen Reader/2—programmed access to the GUI. *Computers for Handicapped Persons*, pp.76–88.

Thayananthan, A. et al., 2003. Shape context and chamfer matching in cluttered scenes. In *Computer Vision and Pattern Recognition, 2003. Proceedings. 2003 IEEE Computer Society Conference on*. p. I–127. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1211346 [Accessed June 23, 2012].

Thompson, S., Johnston, C.J. & Thurlow, M.L., 2002. *Universal design applied to large scale assessments*, National Center on Educational Outcomes Synthesis Report. Available at:

http://osepideasthatwork.org/toolkit/pdf/Universal_Design_LSA.pdf [Accessed July 7, 2012].

Thylefors, B. et al., 1995. Global data on blindness. *Bulletin of the World Health Organization*, 73(1), p.115.

Ticketmaster Inc., 2012. Ticketmaster - About Us. Available at: http://www.ticketmaster.ie/about_us/?tm_link=tm_homeA_i_abouttm [Accessed June 10, 2012].

Tuley, R., 2011. How the textCAPTCHA web service works. Available at: http://textcaptcha.com/how_it_works [Accessed June 23, 2012].

Turing, A.M., 1950. Computing machinery and intelligence. *Mind*, 59(236), pp.433–460.

United Nations Enable, 2004. UN Enable - Human Rights and Disabled Persons 2/6. Available at: http://www.un.org/esa/socdev/enable/dispaperdes1.htm [Accessed July 6, 2012].

University of Cambridge, 2009. Exclusion calculator - Inclusive design tools. *Inclusive Design Toolkit Home*. Available at: http://www.inclusivedesigntoolkit.com/betterdesign2/exclusioncalc/exclusionc alc.html [Accessed May 21, 2012].

Vimina, E. & Areekal, A.U., 2009. Telling computers and humans apart automatically using activity recognition. In *Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on*. pp. 4906–4909.

W3C, 2002. Exploring Usability Enhancements in W3C Process - slide 'Usability - ISO 9241 definition'. Available at: http://www.w3.org/2002/Talks/0104-usabilityprocess/slide3-0.html [Accessed July 8, 2012].

W3C, 2005. Inaccessibility of CAPTCHA. *W3C*. Available at: http://www.w3.org/TR/turingtest/#biometrics [Accessed January 11, 2012].

W3C, 2010. Involving Users in Evaluating Web Accessibility. Available at: http://www.w3.org/WAI/eval/users.html [Accessed May 22, 2012].

WAI, 2011. WCAG Overview. Available at: http://www.w3.org/WAI/intro/wcag.php [Accessed July 7, 2012].

WAI, 2012. Web Accessibility Initiative (WAI) - home page. Available at: http://www.w3.org/WAI/ [Accessed July 7, 2012].

Van Welie, M., Van Der Veer, G.C. & Eliëns, A., 1999. Breaking down usability. In *Proceedings of INTERACT*. pp. 613–620. Available at: http://www.cs.vu.nl/~gerrit/gta/docs/Interact99.pdf [Accessed July 8, 2012].

Whitaker, S. & Porter, J., 2002. Valuing people: a New Strategy for Learning Disability for the 21st Century. *British Journal of Learning Disabilities*, 30(3), pp.133–133.

WHO, 2008. Atlas Multiple Sclerosis. Available at: http://www.who.int/entity/mental_health/neurology/Atlas_MS_WEB.pdf [Accessed July 6, 2012].

WHO, 2012a. WHO | Chronic rheumatic conditions. *WHO*. Available at: http://www.who.int/chp/topics/rheumatic/en/ [Accessed July 6, 2012].

WHO, 2011. WHO | Disability and health. *WHO*. Available at: http://www.who.int/mediacentre/factsheets/fs352/en/index.html [Accessed July 6, 2012].

WHO, 2012b. WHO | Visual impairment and blindness. *WHO*. Available at: http://www.who.int/mediacentre/factsheets/fs282/en/ [Accessed July 6, 2012].

Wildes, R.P., 1997. Iris recognition: an emerging biometric technology. *Proceedings of the IEEE*, 85(9), pp.1348–1363.

Woodward Jr, J.D. et al., 2003. *Biometrics: A look at facial recognition*, DTIC Document. Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA414520 [Accessed June 22, 2012].

World Health Organization, 2001. *International Classification of Functioning, Disability and Health: ICF.*, World Health Organization.

Xiao, Q. & Defence, R.D., 2002. *Trusted User Authentication Using Biometrics*, Defence R&D Canada-Ottawa. Available at: http://pubs.drdc.gc.ca/PDFS/unc26/p518641.pdf [Accessed June 22, 2012].

Yan, J. & El Ahmad, A.S., 2008a. A Low-cost Attack on a Microsoft CAPTCHA. In *Proceedings of the 15th ACM conference on Computer and communications security*. pp. 543–554.

Yan, J. & El Ahmad, A.S., 2008b. Usability of CAPTCHAs or usability issues in CAPTCHA design. In *Proceedings of the 4th symposium on Usable privacy and security*. pp. 44–52.

Zhao, W. et al., 2003. Face recognition: A literature survey. *Acm Computing Surveys (CSUR)*, 35(4), pp.399–458.

# APPENDICES

## APPENDIX A: PROTOTYPING TESTING TRANSCRIPTS

**Interviewer:**     **Anita Foley**

**Tester:**          **Male – 26 yrs old**

**Test Round:**      **1**

| | |
|---|---|
| Interviewer: | Ok you can start |
| Tester: | *press text in grey bar underneath button....* does this not work? |
| Interviewer: | well that's not the button actually |
| Tester: | Oh well I thought that this way the button |
| Interviewer: | what made you think it was the button |
| Tester: | The fact that it's shaded... it just looks like a button |
| Interviewer: | Do you think if I added that shading to the real button on the page you would think it was a button. |
| Tester: | I'm not sure... maybe.... maybe if you added a little bit of a shadow underneath... |
| Interviewer: | Like a drop shadow? |
| Tester: | Yeah exactly. |
| Interviewer: | Ok cool, I can definitely do that. |
| Tester: | *presses face button... lifts iPad up and moves it downward along the face as if to "scan" face.* |
| Interviewer: | *Laughs (a lot)....* why did you do that? |
| Tester: | Well it said scan... |
| Interviewer: | Ok so if the text said place your face in an area you'd understand it better. |
| Tester: | Yeah probably.... |
| Tester: | *selects swipe button... uses three fingers and drags them from one side of the screen to the other... system does not respond...* this isn't working. It's telling me to swipe from left to right... oh you're meant to do it just there? *...points to the modal area...* |
| Interviewer: | yeah yeah you're meant to do it just there |

| | |
|---|---|
| Tester: | ok well that isn't quite clear |
| Interviewer: | what do you think would make it clearer? |
| Tester: | it should explicitly say that it should be done in this area |
| Interviewer: | ok so maybe I'll say swipe your finger in the area below. |
| Tester: | yeah that would be good. |
| Interviewer: | I might change this image to something different |
| Tester: | well I think the image is ok... it's just not that clear where to swipe |
| Interviewer: | ok. |
| Tester: | *selects finger print button... pauses....* I'm not sure in this now if I'm meant to swipe my finger |
| Interviewer: | what do you mean? |
| Tester: | well like on this... *points to fingerprint scanner on laptop...* I need to swipe my finger along it. |
| Interviewer: | oh ok |
| Tester: | but here I'm not sure, although seeing that the fingerprint symbol is there I'd say I just have to press it down |
| Interviewer: | ok |
| Tester: | Ok it worked. |
| Interviewer: | So what do you think would make it clearer? |
| Tester: | If it said press your finger rather than scan your finger. |
| Interviewer: | hmmm... ok. Makes sense |
| Tester: | *selects voice button....* David.... it didn't do anything |
| Interviewer: | yeah I know, it's just a prototype testing the interface... |
| Tester: | oh right |
| Interviewer: | any problem with that screen |
| Tester: | no, I think it's fine. |
| Interviewer: | Ok so a few last questions |
| Tester: | ok |
| Interviewer: | Out of all of these methods, which would be your favourite? |
| Tester: | Probably the swiping one |
| Interviewer: | why is that? |
| Tester: | ah just. It's a lot quicker and easier. |
| Interviewer: | Which is your least favourite? |

| Tester: | Probably the face because it feels a bit weird using the camera |
|---|---|
| Interviewer: | ok cool. Well that's it. Thanks. |

---

| Interviewer: | **Anita Foley** |
|---|---|
| Tester: | **Female - 26 yrs old - Expert User** |
| Test Round: | **2** |

| Interviewer: | Ok you can begin... |
|---|---|
| Tester: | Ok, right, I'll do the gesturing one first... Just any swipe? Anywhere? *Tester swipes* |
| Interviewer: | I mean yeah, so that swipe you did worked. It correctly recognised that you swiped and went to the next page. Is there anything there... *points to screen*.... that I could do there to let you know what why to swipe. |
| Tester: | Yeah well I think you could have an animation that faded out. Maybe a blue line that just goes... *gestures hand left to right on the screen* |
| Interviewer: | Ok so this line would show you what way to go |
| Tester: | Yeah even like a blue circle that faded out, and you could follow it along with your finger. |
| Interviewer: | Oh yeah ok. I like that idea. Let's go back to the main screen again. |
| Tester: | Oh the next one is going to be a doozey, fingerprint right? *Selects finger print button*...Yeah, this is pretty obvious. *Places index finger on the screen.* |
| Interviewer: | Yeah that's fine. |
| Tester: | It just doesn't work yet? |
| Interviewer: | Oh yeah I know it doesn't work but for the prototype... |
| Tester: | yeah yeah |
| Interview: | So you think that's pretty understandable? That you put your finger on the screen? |
| Tester: | yeah. As long as it doesn't matter what finger I use, I can use whatever finger I want, Otherwise I wouldn't know what to do |

124

| | |
|---|---|
| Interviewer: | Yeah, if the text said index finger, you would know what your index finger is? |
| Tester: | Yeah. *Laughs.... selects voice screen*. Yeah ok... so... I get that one |
| Interviewer: | Do you not know your name no? |
| Tester: | laughs. I'm not going to presume that I have to say your name aloud. I can guess I'm meant to say my name. That's pretty obvious |
| Interviewer: | Yeah well I don't want you to say my name... *laughs* |
| Tester: | *laughs.....* Yeah I suppose that pretty self explanatory..... *Selects face recognition button...* And then the face one. |
| Interviewer: | Obviously in an ideal world I'd have a camera here that would show your face |
| Tester: | So I don't have to mash my face into in no? |
| Interviewer: | Ha no. So this screen makes sense. |
| Tester: | he...let me see, see in a real world I presume the real application is here... *points to the screen in the background...* and so this box here... *points to the picture of the human face...* would show my face? |
| Interviewer: | Yeah exactly. It would look like your taking a picture of yourself. |
| Tester: | Ok so this picture wouldn't be here. |
| Interviewer: | Exactly. |
| Tester: | Ok that would make sense. So I'd presume... well it would be nice to... I don't know if this is possible, but for the box to be red, and then when you had your face right in the box would turn green. |
| Interviewer: | Oh yeah yeah. Oh that's very good Kevin. |
| Tester: | Ok so I think that's pretty good.... *goes back to main screen* |
| Interviewer: | So anything on that screen that you'd like to change. |
| Tester: | This one? Well this isn't part of the application is it? Erma... I didn't know what this was until you told me. I didn't know what gesture, fingerprint, voice and face are going to do. |
| Interviewer: | yeah ok, so I have to have some instruction there. |

| | |
|---|---|
| Tester: | Like CAPTCHA always has a thing saying fill in this box. I know my dad will just read that and then do whatever it tells him to. It doesn't tell the user why, users just do it |
| Interviewer: | So if I said select your preferred input, you'd understand what that meant? |
| Tester: | Yeah. I also think that if I was presented with this screen I'd pick gesture each time. |
| Interviewer: | why is that? |
| Tester: | Just it's easier and quicker and I know it'll work. I don't want to have to speak out loud cause that's annoying. Face thing I'd have to align it, Fingerprint software can be unreliable. So I'd pick gesture every time |
| Interviewer: | So if there setting where you could pick your preferred input you'd select gesture. Then you would no longer get this screen. They could be brought straight to the gesturing screen |
| Tester: | Yeah I'd do that. |
| Interviewer: | Ok cool. That's it. |

---

| | |
|---|---|
| **Interviewer:** | **Anita Foley** |
| **Tester:** | **Male – 24 yrs old – English Not First Language** |
| **Test Round:** | **3** |

| | |
|---|---|
| Tester: | *selects swipe button... it swipes correctly.* |
| Interviewer: | Yeah so you got that working with the first pass. |
| Tester: | Ok. *Selects fingerprint button... Places finger on screen.* |
| Interviewer: | Yeah that's prefect. |
| Tester: | *selects voice button* |
| Tester: | *pauses.... brings iPad close to mouth and laughs* |
| Interviewer: | Ok so the idea there is that you would say your name |
| Tester: | Yes yeah say my name... *Selects face button... pauses...* |
| Interviewer: | If there was a camera view there would you know what to do. |
| Tester: | yes... *turns iPad to portrait view (as before it was landscape)* |
| Interviewer: | That's interesting, the way you turned the iPad. |

| | |
|---|---|
| Tester: | Because if I held it like this my thumb would be in the way of the camera. |
| Interviewer: | Oh yes I see, I hadn't thought of that. So if there anything on the main screen you'd change? |
| Tester: | So all these buttons do the same actions, but in different ways? |
| Interviewer: | Yes |
| Tester: | Hmmm...It's only for authentication? |
| Interviewer: | It's to test if you are a human. Doesn't matter about your password or username or anything. |
| Tester: | Ok ok, just to test if you are human. So I need to select these four options |
| Interviewer: | you only need to select one |
| Tester: | Yeah, what if the device does not support one of these inputs. Maybe this option should not appear. |
| Interviewer: | Yeah that's interesting. Maybe I could even show it disabled. If you were using this software which input type would you prefer? |
| Tester: | This one... *points to gesture* |
| Interviewer: | why that one? |
| Tester: | Because it's easier |
| Interviewer: | What would your second option be? |
| Tester: | This one... *points to the face option....* because I don't need to s peak. |
| Interviewer: | Yea yeah makes sense. Ok cool. That's it. |

| | |
|---|---|
| **Interviewer:** | **Anita Foley** |
| **Tester:** | **Male – 33 – Expert User** |
| **Test Round:** | **4** |
| | |
| Tester: | *selects login button.... reads text out loud... selects gesture.... reads text out aloud.... swipes finger.* |
| Interviewer: | Perfect. So that's the first input type done. From here you would then continue to log in. So you were happy with that process |

| | |
|---|---|
| Tester: | eh yeah it was straight forward enough. No problem at all. It's grand. |
| Interviewer: | Ok you can go ahead now and pick a different option |
| Tester: | *selects fingerprint... reads text aloud... places finger....* test what finger though in the area below? |
| Interviewer: | You'd prefer it to specify? |
| Tester: | Yeah. |
| Interviewer: | Ok that makes sense. I've had a few people saying that. |
| Tester: | *Selects voice.... pauses.....* Yeah ok... *laugh...* my big thing with that is, you wouldn't feel comfortable working, like... |
| Interviewer: | yeah you'd feel a bit awkward, talking out loud... |
| Tester: | in work, yeah. |
| Interviewer: | yeah |
| Tester: | The face one now. *Reads out text...* so this obviously turns on the camera does it? |
| Interviewer: | Yeah so you'd understand what to do. In real life you'd want that screen to reflect what the front facing camera was seeing. |
| Tester: | yeah that would work. That would be no problem for me. You'd just be worried about what effect the orientation of your face and the light and thing |
| Interviewer: | yeah |
| Tester: | Yeah good work. I don't have a problem with it. Overall it has clear instructions and it's straight forward enough really, just say what finger you want scanned... that's the only thing of note. |
| Interviewer: | Ok cool. Let me ask you a few questions then. The text here at the top, that makes sense to you? |
| Tester: | It does it does. Probably is needed, but to be honest I didn't read it until now. |
| Interviewer: | Yeah, that's a good point. Maybe it needs to be made more prominent for novice users so they can see it... obviously we would ignore it to be fair |
| Tester: | I'd change it to... you can log in by... gesture, fingerprint, voice, face |

| Interviewer: | Oh yeah yeah that's good. You're always good with the words Pat |
|---|---|
| Tester: | I do try Anita. |
| Interviewer: | if you had a preference of these options, which one would you pick? |
| Tester: | eh... gesture, because of my HTC. Oh maybe the finger print one because it's more secure |
| Interviewer: | what would be your second? |
| Tester: | gesture even though I think it's not as secure. The face one... I mean... I spend enough time looking in the mirror, so I don't need that. The fingerprint is definitely the best one. Or even a whole palm print. |
| Interviewer: | Yeah that's an interesting point. I could try that. Ok that's it, thank you. |

---

| Interviewer: | **Anita Foley** |
|---|---|
| Tester: | **Male – 48 yrs old - Intermediate User** |
| Test Round: | **5** |

| Interviewer: | ok you can start |
|---|---|
| Tester: | *selects gesture, swipes* |
| Interviewer: | oh that's it. That's fine. Select another option... |
| Tester: | ok. *Selects finger print.* |
| Interviewer: | Perfect, you're the first person to get working first time. Ok so you're ok with that text? |
| Tester: | Yeah no it's grand. Oh I have to do them all? *Selects voice...* PADRAIG |
| Interviewer: | That's perfect. It doesn't actually recognise your voice yet. So you're happy with that then? Happy with the text? |
| Tester: | Yeah yeah. *Selects face...* should...emm there be something to press... like a camera button on the end. Cause when you see it might make it clearer when you're done |
| Interviewer: | yeah that makes sense. I could do that. |

| Tester: | I think once you see the camera looking at yeah it would make more sense. And you know I'd probably prefer it that way... *turns iPad portrait* |
|---|---|
| Interviewer: | Yeah. You're not the first person to suggest that actually. |
| Tester: | yeah because the camera is there |
| Interviewer: | yeah absolutely. So if you were to pick one of these as a preference, which one would you pick. |
| Tester: | this one... *points to gesture* |
| Interviewer: | and why that one? |
| Tester: | arm. It's just the interface I'm used to with this type of device. Cause it's all fingers and y'know. |
| Interviewer: | If you had a second preference what would it be? |
| Tester: | Erma... I think probably the voice |
| Interviewer: | and why? |
| Tester: | I dunno... it's just the finger print seems a bit too secure. the face... ehhh I dunno, I don't like getting my picture taken |
| Interviewer: | ha ha yeah. Cool. That's prefect. Thanks. |

---

| **Tester:** | **Male – 34 yrs old - Dyslexic** |
|---|---|
| **Test Round:** | **6** |
| | |
| Tester: | *selects login button.* Do I have to? I mean does it matter what I pick? ...*points to all the options* |
| Interviewer: | No |
| Tester: | *selects fingerprint.. places middle finger down...* |
| Interviewer: | ok so I notice you placed your middle finger down |
| Tester: | looks down at iPad again... oh yeah yeah I didn't read it... *points to the text* |
| Interviewer: | ok that's fine |
| Tester: | Yeah no I didn't read it. Cause like if you see a fingerprint you just know what to do |
| Interviewer: | Yeah. I suppose people have different preference of which finger they like to use |

| | |
|---|---|
| Tester: | *selects gesture... pauses... swipes....* |
| Interviewer: | Any problem with that? |
| Tester: | Well no. I know to read the instructions now.... |
| Interviewer: | Oh well you don't have to read it, you can do whatever you want. If you want to not read it that's fine. It's all about user interaction. |
| Tester: | Ok... *selects voice button....* Mark. |
| Interviewer: | Ok cool. Obviously it doesn't have anything happening it the background yet. But that's ok. So you understood? |
| Tester: | Yeah |
| Interviewer: | Cool, next |
| Tester: | *selects face button... turns iPad portrait. Hits camera button.* |
| Interviewer: | yeah that's fine. Perfect. A lot of people are doing that... |
| Tester: | what? What am I doing? |
| Interviewer: | turning the iPad around |
| Tester: | Oh yeah, but sure that's where the camera is... points to camera... |
| Interviewer: | Oh yeah I know... I just hadn't thought of that before... |
| Tester: | oh right... |
| Interviewer: you do like? | any problem with that page, anything you don't like, anything |
| Tester: | eh well the orientation of the camera. And it doesn't look like the app.... when you're taken a photo, it doesn't look like the photo app. |
| Interviewer: | Oh yeah I know what you mean. It'd be good if the image would take up all the whitespace |
| Tester: | Yeah because the only thing that threw me off initially was the grey bar going around it. Other than that no it's good. |
| Interviewer: | so, out of those 4 options, which one would you prefer? |
| Tester: | prefer for what? |
| Interviewer: | if this was the way you had to log into an application each time. Which would be your preferred approach? |
| Tester: | well... the gesture makes more sense. |
| Interviewer: | why does it make more sense? |

| | |
|---|---|
| Tester: | well just you can access it from anywhere. Definitely not the voice cause I don't want people hearing me. Eh... the face would be ok. Ehh... I actually think the face would require the least amount of work. |
| Interviewer: | the least amount? |
| Tester: | yeah. I shouldn't have to do anything. I should just be able to walk up to it and done. So that makes more sense. I don't want to put my fingerprint up |
| Interviewer: | why don't you want to put your fingerprint ? |
| Tester: | because you could leave a mark on the screen and people could scam it. So I think the face to me would be the most secure and least amount of interaction required |
| Interviewer: | ok cool, so anything else you want to add? |
| Tester: | oh ok. So was that an all-star performance? |
| Interviewer: | absolutely. That's it, brilliant |

## APPENDIX B: ICF MATRIX FOR BIOMETRIC INTERACTION

| Score | Description |
|---|---|
| 0 | No Impairment |
| 1 | Mild |
| 2 | Moderate |
| 3 | Severe |
| 4 | Complete |

| Body Functional Factors | Face | Voice | Hand writing | Finger print | Retina |
|---|---|---|---|---|---|
| b1. MENTAL FUNCTIONS | | | | | |
| b110 Consciousness | 4 | 4 | 4 | 4 | 4 |
| b114 Orientation    (time, place, person) | 2 | 4 | 2 | 1 | 2 |
| b117 Intellectual   ( incl. Retardation, dementia) | 1 | 3 | 3 | 3 | 3 |
| b130 Energy and drive functions | 3 | 0 | 0 | 0 | 0 |
| b134 Sleep | 0 | 0 | 0 | 0 | 0 |
| b140 Attention | 1 | 1 | 1 | 1 | 1 |
| b144 Memory | 1 | 2 | 1 | 0 | 0 |
| b152 Emotional functions | 0 | 0 | 0 | 0 | 0 |
| b156 Perceptual functions | 0 | 0 | 0 | 0 | 0 |
| b164 Higher level cognitive functions | 3 | 2 | 2 | 2 | 2 |
| b167 Language | 1 | 4 | 3 | 0 | 0 |
| b2. SENSORY FUNCTIONS AND PAIN | | | | | |
| b210 Seeing | 4 | 0 | 4 | 2 | 4 |
| b230 Hearing | 0 | 1 | 0 | 0 | 0 |
| b235 Vestibular   (incl. Balance functions) | 1 | 0 | 0 | 0 | 0 |
| b280 Pain | 2 | 0 | 1 | 1 | 1 |
| b3. VOICE AND SPEECH FUNCTIONS | | | | | |
| b310 Voice | 0 | 4 | 0 | 0 | 0 |
| b4. FUNCTIONS OF THE CARDIOVASCULAR, | | | | | |

| HAEMATOLOGICAL, IMMUNOLOGICAL AND RESPIRATORY SYSTEMS | | | | | |
|---|---|---|---|---|---|
| b410 Heart | 0 | 0 | 0 | 0 | 0 |
| b420 Blood pressure | 0 | 0 | 0 | 0 | 0 |
| b430 Haematological  (blood) | 0 | 0 | 0 | 0 | 0 |
| b435 Immunological (allergies, hypersensitivity) | 0 | 0 | 0 | 0 | 0 |
| b440 Respiration (breathing) | 0 | 3 | 0 | 0 | 0 |
| b5. FUNCTIONS OF THE DIGESTIVE, METABOLIC AND ENDOCRINE SYSTEMS | | | | | |
| b515 Digestive | 0 | 0 | 0 | 0 | 0 |
| b525 Defecation | 0 | 0 | 0 | 0 | 0 |
| b530 Weight maintenance | 0 | 0 | 0 | 0 | 0 |
| b555 Endocrine glands (hormonal changes) | 0 | 0 | 0 | 0 | 0 |
| b6. GENITOURINARY AND REPRODUCTIVE FUNCTIONS | | | | | |
| b620 Urination | 0 | 0 | 0 | 0 | 0 |
| b640 Sexual functions | 0 | 0 | 0 | 0 | 0 |
| b7. NEUROMUSCULOSKELETAL AND MOVEMENT  RELATED FUNCTIONS | | | | | |
| b710 Mobility of joint | 3 | 0 | 3 | 3 | 3 |
| b730 Muscle power | 3 | 0 | 2 | 1 | 3 |
| b735 Muscle tone | 1 | 0 | 1 | 0 | 1 |
| b765 Involuntary movements | 3 | 0 | 3 | 3 | 3 |
| b8. FUNCTIONS OF THE SKIN AND RELATED STRUCTURES | 0 | 0 | 1 | 3 | 0 |
| **Body Structure Factors** | **Face** | **Voice** | **Hand writing** | | |
| s1. STRUCTURE OF THE NERVOUS SYSTEM | | | | | |
| s110 Brain | 3 | 3 | 3 | 3 | 3 |
| s120 Spinal cord and peripheral nerves | 4 | 2 | 3 | 3 | 3 |
| s2. THE EYE, EAR AND RELATED STRUCTURES | 3 | 0 | 0 | 0 | 4 |
| s3. STRUCTURES INVOLVED IN VOICE AND SPEECH | 0 | 4 | 0 | 0 | 0 |

| | Face | Voice | Hand writing | | |
|---|---|---|---|---|---|
| s4. STRUCTURE OF THE CARDIOVASCULAR, IMMUNOLOGICAL AND RESPIRATORY SYSTEMS | 0 | 3 | 0 | 0 | 0 |
| s410 Cardiovascular system | 0 | 0 | 0 | 0 | 2 |
| s430 Respiratory system | 0 | 3 | 0 | 0 | 0 |
| s5. STRUCTURES RELATED TO THE DIGESTIVE, METABOLISM AND ENDOCRINE SYSTEMS | 0 | 0 | 0 | 0 | 0 |
| s6. STRUCTURE RELATED TO GENITOURINARY AND REPRODUCTIVE SYSTEM | 0 | 0 | 0 | 0 | 0 |
| s610 Urinary system | 0 | 0 | 0 | 0 | 0 |
| s630 Reproductive system | 0 | 0 | 0 | 0 | 0 |
| s7. STRUCTURE RELATED TO MOVEMENT | | | | | |
| s710 Head and neck region | 3 | 0 | 0 | 0 | 3 |
| s720 Shoulder region | 2 | 0 | 1 | 0 | 2 |
| s730 Upper extremity (arm, hand) | 3 | 1 | 3 | 3 | 3 |
| s740 Pelvis | 0 | 0 | 0 | 0 | 0 |
| s750 Lower extremity (leg, foot) | 0 | 0 | 0 | 0 | 0 |
| s760 Trunk | 0 | 0 | 0 | 0 | 0 |
| s8. SKIN AND RELATED STRUCTURES | 1 | 0 | 1 | 3 | 0 |
| **Activity and Participation Factors** | **Face** | **Voice** | **Hand writing** | | |
| d1. LEARNING AND APPLYING KNOWLEDGE | | | | | |
| d110 Watching | 3 | 1 | 1 | 1 | 3 |
| d115 Listening | 0 | 0 | 0 | 0 | 0 |
| d140 Learning to read | 0 | 0 | 0 | 0 | 0 |
| d145 Learning to write | 0 | 0 | 4 | 0 | 0 |
| d150 Learning to calculate (arithmetic) | 0 | 0 | 0 | 0 | 0 |
| d175 Solving problems | 0 | 0 | 0 | 0 | 0 |
| d2. GENERAL TASKS AND DEMANDS | | | | | |
| d210 Undertaking a single task | 1 | 1 | 1 | 1 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| d220 Undertaking multiple tasks | 1 | 1 | 1 | 1 | 1 |
| **d3. COMMUNICATION** | | | | | |
| d310 Communicating with -- receiving -- spoken messages | 0 | 3 | 0 | 0 | 0 |
| d315 Communicating with -- receiving -- non-verbal messages | 2 | 3 | 2 | 0 | 0 |
| d330 Speaking | 0 | 4 | 0 | 0 | 0 |
| d335 Producing non-verbal messages | 0 | 0 | 2 | 0 | 0 |
| d350 Conversation | 0 | 2 | 0 | 0 | 0 |
| **d4. MOBILITY** | | | | | |
| d430 Lifting and carrying objects | 3 | 0 | 0 | 0 | 3 |
| d440 Fine hand use (picking up, grasping) | 3 | 0 | 4 | 2 | 3 |
| d450 Walking | 0 | 0 | 0 | 0 | 0 |
| d465 Moving around using equipment (wheelchair, skates, etc.) | 0 | 0 | 0 | 0 | 0 |
| d470 Using transportation (car, bus, train, plane, etc.) | 0 | 0 | 0 | 0 | 0 |
| d475 Driving  (riding bicycle and motorbike, driving car, etc.) | 0 | 0 | 0 | 0 | 0 |
| **d5. SELF CARE** | | | | | |
| d510 Washing oneself    (bathing, drying, washing hands, etc) | 0 | 0 | 0 | 0 | 0 |
| d520 Caring for body parts   (brushing teeth, shaving, grooming, etc.) | 0 | 0 | 0 | 0 | 0 |
| d530 Toileting | 0 | 0 | 0 | 0 | 0 |
| d540 Dressing | 0 | 0 | 0 | 0 | 0 |
| d550 Eating | 0 | 0 | 0 | 0 | 0 |
| d560 Drinking | 0 | 0 | 0 | 0 | 0 |
| d570 Looking after one`s health | 0 | 0 | 0 | 0 | 0 |
| **d6. DOMESTIC LIFE** | | | | | |
| d620 Acquisition of goods and services (shopping, etc.) | 0 | 0 | 0 | 0 | 0 |
| d640 Doing housework (cleaning house, washing dishes laundry, ironing, etc.) | 0 | 0 | 0 | 0 | 0 |
| d630 Preparation of meals  (cooking etc.) | 0 | 0 | 0 | 0 | 0 |
| d660 Assisting others | 0 | 0 | 0 | 0 | 0 |
| **d7. INTERPERSONAL INTERACTIONS AND RELATIONSHIPS** | | | | | |

| | Face | Voice | Hand writing | | |
|---|---|---|---|---|---|
| d710 Basic interpersonal interactions | 0 | 0 | 0 | 0 | 0 |
| d720 Complex interpersonal interactions | 0 | 0 | 0 | 0 | 0 |
| d730 Relating with strangers | 0 | 0 | 0 | 0 | 0 |
| d740 Formal relationships | 0 | 0 | 0 | 0 | 0 |
| d750 Informal social relationships | 0 | 0 | 0 | 0 | 0 |
| d760 Family relationships | 0 | 0 | 0 | 0 | 0 |
| d770 Intimate relationships | 0 | 0 | 0 | 0 | 0 |
| **Environmental Factor** | **Face** | **Voice** | **Hand writing** | | |
| e1. PRODUCTS AND TECHNOLOGY | | | | | |
| e110 For personal consumption (food, medicines) | 0 | 0 | 0 | 0 | 0 |
| e115 For personal use in daily living | 0 | 0 | 0 | 0 | 0 |
| e120 For personal indoor and outdoor mobility and transportation | 0 | 0 | 0 | 0 | 0 |
| e125 Products for communication | 0 | 0 | 1 | 0 | 0 |
| e150 Design, construction and building products and technology of buildings for public use | 0 | 0 | 0 | 0 | 0 |
| e155 Design, construction and building products and technology of buildings for private use | 0 | 0 | 0 | 0 | 0 |
| e2. NATURAL ENVIRONMENT AND HUMAN MADE CHANGES TO ENVIRONMENT | | | | | |
| e225 Climate | 1 | 1 | 1 | 1 | 1 |
| e240 Light | 3 | 1 | 2 | 0 | 4 |
| e250 Sound | 0 | 4 | 0 | 0 | 0 |
| e3. SUPPORT AND RELATIONSHIPS | | | | | |
| e310 Immediate family | 0 | 0 | 0 | 0 | 0 |
| e320 Friends | 0 | 0 | 0 | 0 | 0 |
| e325 Acquaintances, peers, colleagues, neighbours and community members | 0 | 0 | 0 | 0 | 0 |
| e330 People in position of authority | 0 | 0 | 0 | 0 | 0 |
| e340 Personal care providers and personal assistants | 0 | 0 | 0 | 0 | 0 |
| e355 Health professionals | 0 | 0 | 0 | 0 | 0 |
| e360 Health related professionals | 0 | 0 | 0 | 0 | 0 |

| e4. ATTITUDES | | | | | |
|---|---|---|---|---|---|
| e410 Individual attitudes of immediate family members | 0 | 0 | 0 | 0 | 0 |
| e420 Individual attitudes of friends | 0 | 0 | 0 | 0 | 0 |
| e440 Individual attitudes of personal care providers and personal assistants | 0 | 0 | 0 | 0 | 0 |
| e450 Individual attitudes of health professionals | 0 | 0 | 0 | 0 | 0 |
| e455 Individual attitudes of health related professionals | 0 | 0 | 0 | 0 | 0 |
| e460 Societal attitudes | 0 | 0 | 0 | 0 | 0 |
| e465 Social norms, practices and ideologies | 0 | 0 | 0 | 0 | 0 |
| E5. SERVICES, SYSTEMS AND POLICIES | | | | | |
| e525 Housing services, systems and policies | 0 | 0 | 0 | 0 | 0 |
| e535 Communication services, systems and policies | 1 | 1 | 1 | 1 | 1 |
| e540 Transportation services, systems and policies | 0 | 0 | 0 | 0 | 0 |
| e550 Legal services, systems and policies | 0 | 0 | 0 | 0 | 0 |
| e570 Social security, services, systems and policies | 0 | 0 | 0 | 0 | 0 |
| e575 General social support services, systems and policies | 0 | 0 | 0 | 0 | 0 |
| e580 Health services, systems and policies | 0 | 0 | 0 | 0 | 0 |
| e585 Education and training services, systems and policies | 1 | 1 | 0 | 0 | 0 |
| e590 Labour and employment services, systems and policies | 0 | 0 | 0 | 0 | 0 |

## Text Based CAPTCHA Time Results

| | First Attempt | Second Attempt | Third Attempt |
|---|---|---|---|
| Tester A (MF) | 00:32 | 00:41 | 00:43 |
| Tester B (BF) | 00:36 | 00:25 | 00:12 |
| Tester C (DM) | 00:15 | 00:30 | 00:19 |
| Tester D (KW) | 00:13 | 00:13 | 00:20 |
| Tester E (JY) | 00:22 | 00:29 | 00:18 |
| Tester F (MC) | 00:27 | 00:35 | 00:42 |
| Tester G (PG) | 00:25 | 00:18 | 00:20 |
| Tester H (PR) | 00:28 | 00:20 | 00:15 |
| Tester I (SD) | 00:29 | 00:13 | 00:23 |

## Text Based CAPTCHA Failure Rate

Fail 19%

Pass 81%
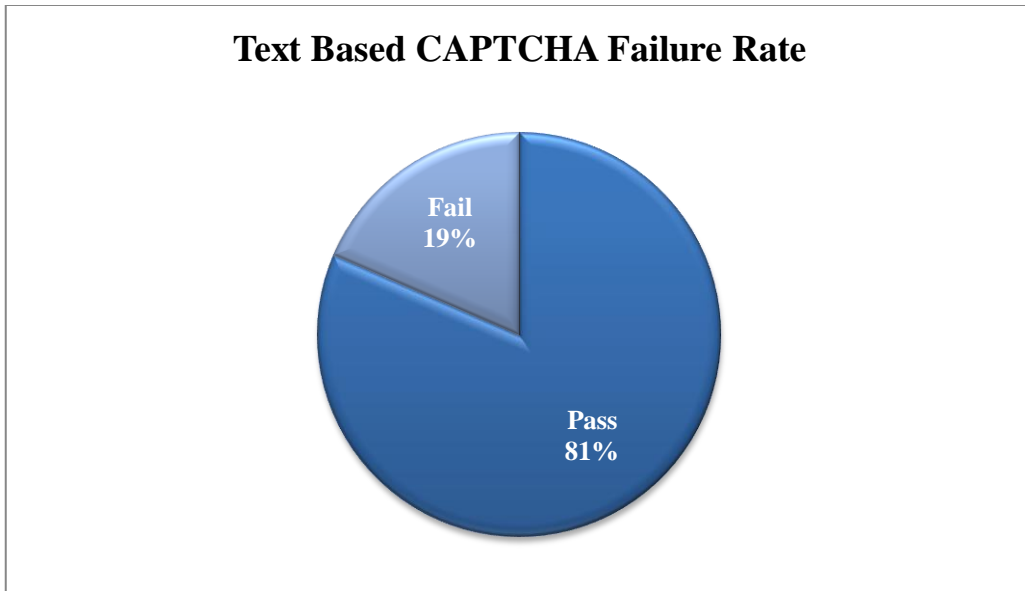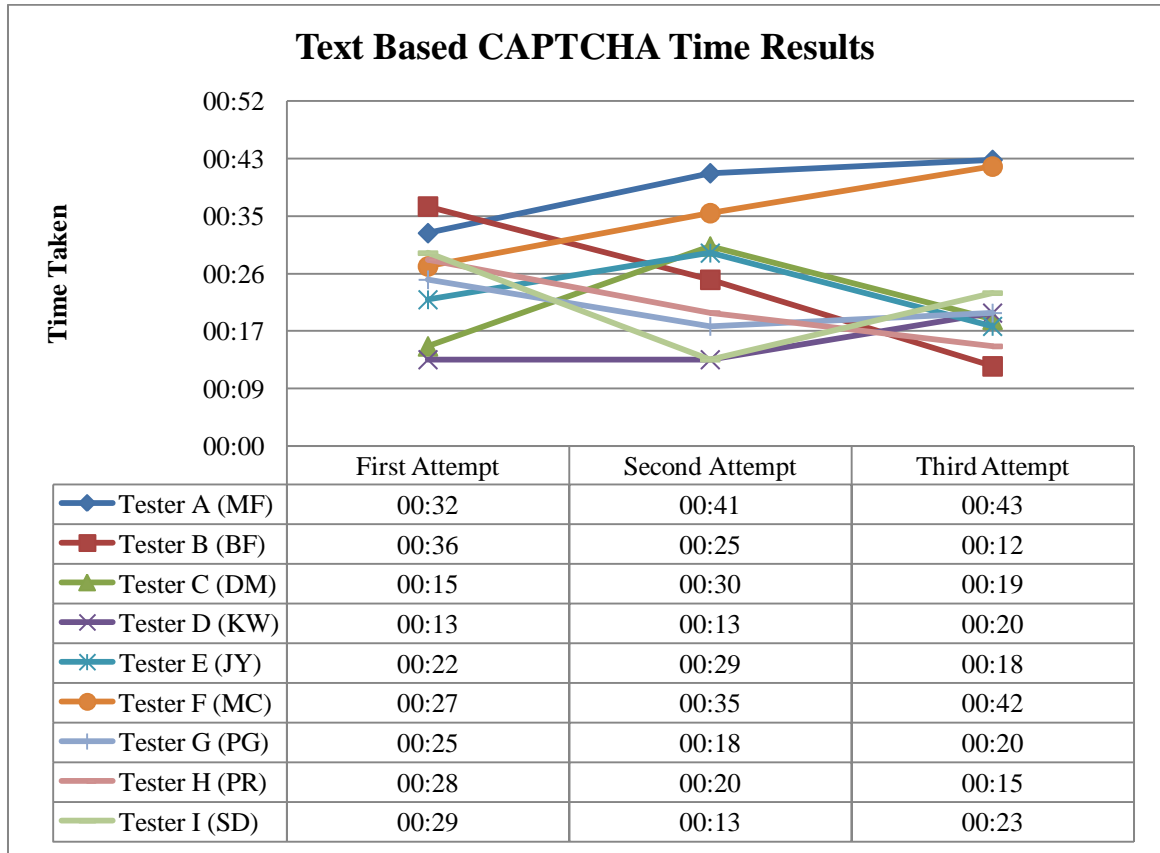
## Audio Based CAPTCHA Time Results
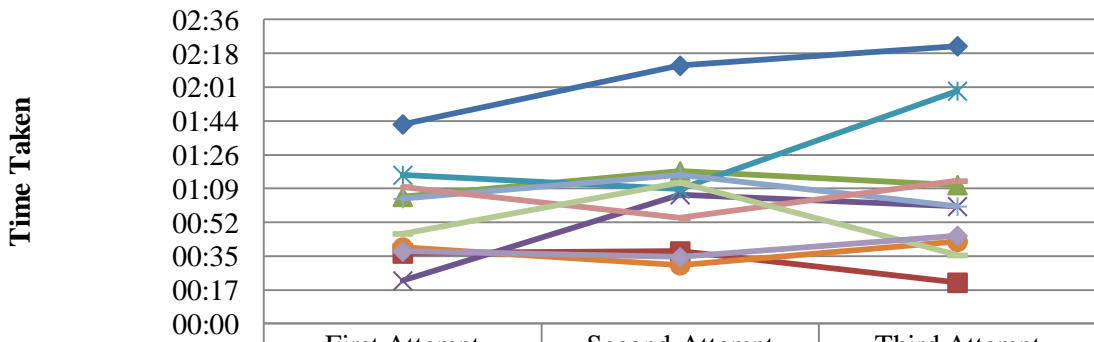


| | First Attempt | Second Attempt | Third Attempt |
|---|---|---|---|
| Tester A (MF) | 01:42 | 02:12 | 02:22 |
| Tester B (BF) | 00:36 | 00:37 | 00:21 |
| Tester C (DM) | 01:05 | 01:18 | 01:11 |
| Tester D (KW) | 00:22 | 01:06 | 01:00 |
| Tester E (JY) | 01:16 | 01:09 | 01:59 |
| Tester F (MC) | 00:39 | 00:30 | 00:42 |
| Tester G (PG) | 01:04 | 01:16 | 01:00 |
| Tester H (PR) | 01:10 | 00:54 | 01:13 |
| Tester I (SD) | 00:46 | 01:12 | 00:35 |
| Tester J (DF) | 00:37 | 00:34 | 00:45 |

## Audio Based CAPTCHA Failure Rate



Pass 4%

Fail 97%
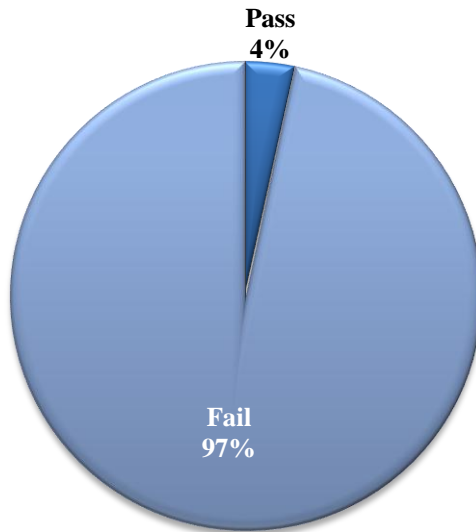
## Time Results - Voice - BioScope
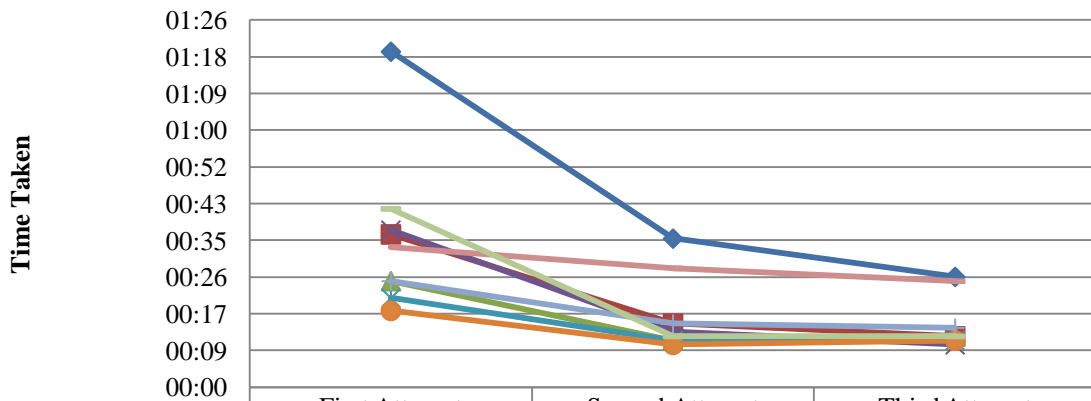


| | First Attempt | Second Attempt | Third Attempt |
|---|---|---|---|
| Tester A (MF) | 01:19 | 00:35 | 00:26 |
| Tester B (BF) | 00:36 | 00:15 | 00:12 |
| Tester C (DM) | 00:25 | 00:11 | 00:12 |
| Tester D (KW) | 00:37 | 00:13 | 00:10 |
| Tester E (JY) | 00:21 | 00:11 | 00:11 |
| Tester F (MC) | 00:18 | 00:10 | 00:11 |
| Tester G (PG) | 00:25 | 00:15 | 00:14 |
| Tester H (PR) | 00:33 | 00:28 | 00:25 |
| Tester I (SD) | 00:42 | 00:12 | 00:12 |

## Time Results - Handwriting - BioScope
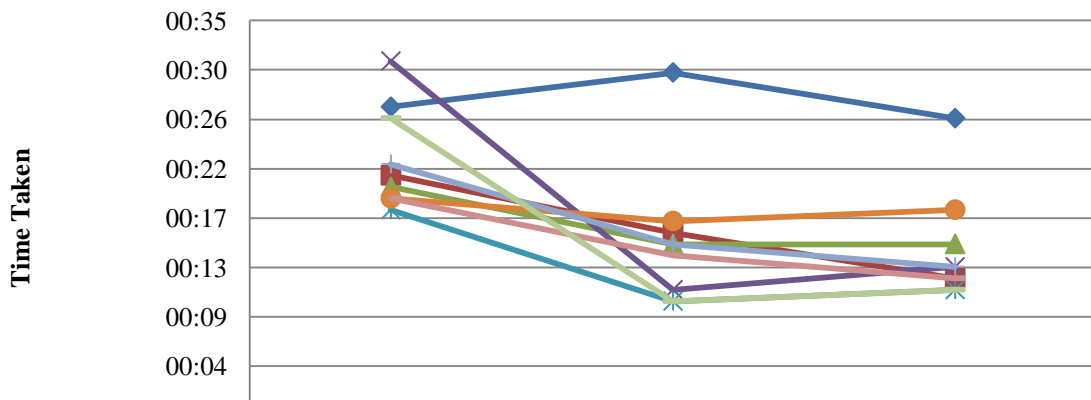


| | First Attempt | Second Attempt | Third Attempt |
|---|---|---|---|
| Tester A (MF) | 00:27 | 00:30 | 00:26 |
| Tester B (BF) | 00:21 | 00:16 | 00:12 |
| Tester C (DM) | 00:20 | 00:15 | 00:15 |
| Tester D (KW) | 00:31 | 00:11 | 00:13 |
| Tester E (JY) | 00:18 | 00:10 | 00:11 |
| Tester F (MC) | 00:19 | 00:17 | 00:18 |
| Tester G (PG) | 00:22 | 00:15 | 00:13 |
| Tester H (PR) | 00:19 | 00:14 | 00:12 |
| Tester I (SD) | 00:26 | 00:10 | 00:11 |

## APPENDIX D: BIOMETRIC PRIVACY SURVEY



**Fingerprint Storage**

Neiter ▪ The Government ▪ Google

I would allow _____ to store my fingerprint if it was required to create an online account?
- 38
- 19
- 17

I would allow _____ to store my fingerprint to use for account creation purposes if it could be used as an alternative to presenting you with a…
- 40
- 16
- 17

I would allow _____ to store my fingerprint to use for login purposes if it could be used as an alternative to typing in my username and…
- 39
- 19
- 15

I would allow _____ to store my fingerprint to use for login purposes if it would reduce the possibility of my account being hacked?
- 37
- 19
- 17



**Voice Information**

Neiter ▪ The Government ▪ Google

I would allow _____ to store a recording of my voice if it was required to create an online account?
- 32
- 26
- 25

I would allow _____ to store a recording of my voice to use for account creation purposes if it could be used as an alternative to presenting…
- 36
- 21
- 23

I would allow _____ to store a recording of my voice to use for login purposes if it could be used as an alternative to typing in my username and…
- 35
- 21
- 24

I would allow _____ to store a recording of my voice to use for login purposes if it would reduce the possibility of my account being hacked?
- 30
- 26
- 27

# Face Information

I would allow _____ to store a picture of my face if it was required to create an online account?
- Neiter: 33
- The Government: 26
- Google: 24

I would allow _____ to store a picture of my face to use for account creation purposes if it could be used as an alternative to presenting you with a...
- Neiter: 37
- The Government: 22
- Google: 21

I would allow _____ to store a picture of my face to use for login purposes if it could be used as an alternative to typing in my username and...
- Neiter: 36
- The Government: 23
- Google: 20

I would allow _____ to store a picture of my face to use for login purposes if it would reduce the possibility of my account being hacked?
- Neiter: 32
- The Government: 27
- Google: 24

# Iris Information

Neiter   The Government   Google

I would allow _____ to store a picture of my iris if it was required to create an online account?
- Neiter: 32
- The Government: 25
- Google: 22

I would allow _____ to store a picture of my iris to use for account creation purposes if it could be used as an alternative to presenting you with a...
- Neiter: 38
- The Government: 19
- Google: 17

I would allow _____ to store a picture of my iris to use for login purposes if it could be used as an alternative to typing in my username and...
- Neiter: 38
- The Government: 19
- Google: 18

I would allow _____ to store a picture of my iris to use for login purposes if it would reduce the possibility of my account being hacked?
- Neiter: 35
- The Government: 23
- Google: 20

# Handwriting Information



Legend: Neiter (green) · The Government (red) · Google (blue)

| Question | Neiter | The Government | Google |
|---|---|---|---|
| I would allow _____ to store a sample of my handwriting if it was required to create an online account? | 32 | 26 | 23 |
| I would allow _____ to store a sample of my handwriting to use for account creation purposes if it could be used as an alternative to… | 34 | 24 | 24 |
| I would allow _____ to store a sample of my handwriting to use for login purposes if it could be used as an alternative to typing in my username… | 34 | 24 | 23 |
| I would allow _____ to store a sample of my handwriting to use for login purposes if it would reduce the possibility of my account being… | 31 | 27 | 25 |

144

**APPENDIX E: CAPTCHA SURVEY RESULTS**

## What age are you?

| Age | Count |
|-----|-------|
| 15-20 | 3 |
| 21-25 | 12 |
| 26-30 | 17 |
| 31-35 | 20 |
| 36-40 | 8 |
| 41-45 | 5 |
| 46-50 | 2 |
| 51-55 | 0 |
| 56-60 | 1 |
| 61-70 | 2 |

## What gender are you?

| Gender | Count |
|--------|-------|
| Female | 21 |
| Male | 49 |

## Which of the following electronic devices do you own?

| Device | Count |
|--------|-------|
| Computer Microphone | 34 |
| Webcam | 43 |
| Music Device | 42 |
| Mobile Phone | 21 |
| Smart Phone | 61 |
| Tablet | 23 |
| PDA | 5 |
| Laptop Computer | 61 |
| Desktop Computer | 36 |

## How many hours each week do you normally spend using an electronic device?

| | |
|---|---|
| More than 20 hours | 44 |
| 16-20 hours | 7 |
| 11-15 hours | 6 |
| 6-10 hours | 8 |
| 3-5 hours | 4 |
| 1-2 hours | 0 |
| Less than an hour | 1 |
| Do not use | 0 |

## Select the following activities that you have performed on a computer

| | |
|---|---|
| Developing computer software | 41 |
| Developing a website | 39 |
| Online Shopping | 63 |
| Surfing the Internet | 70 |
| Downloading or listening to music | 59 |
| Playing computer games | 51 |
| Creating a presentation in PowerPoint | 53 |
| Creating a macro in Microsoft Excel | 32 |
| Reading, writing a document in Microsoft Word | 67 |
| Reading, writing or sending an email | 70 |

## Which of the following concern you regarding information technology

| | |
|---|---|
| Spam | 25 |
| Computer Viruses, worms or trojan horses | 34 |
| My technical skill level in troubleshooting my… | 21 |
| Slow or inadequate Internet access | 56 |
| The age of your computer hardware and software | 28 |

*__Other Responses:__*

"Privacy"

"The increasing role that censorship is starting to play in access to the internet."

"Ability of device to carry out the tasks I want in a timely manner"

"Privacy"

"The Man"

"As IT is now very much part of day to day life I would be concerned with the health issues surrounding some aspects of it. E.g. Eye Sight, Radiation, Anti-social. Also concerned with privacy in IT."

"What other technology is out there so I can see what its does and what I can make it do (hack it)"

"Battling Windows Server entropy...."

"Machine speed"

"The government"

**Have you ever completed a CAPTCHA test before?**

| Response | Count |
| --- | --- |
| No | 6 |
| Yes | 62 |

**If yes, what were you trying to do on the Internet at the time?**

| Activity | Count |
| --- | --- |
| Buying a ticket for an event | 55 |
| Creating user account | 50 |
| Adding comment to a blog | 27 |
| Logging into social networking site | 28 |
| Logging into email account | 39 |
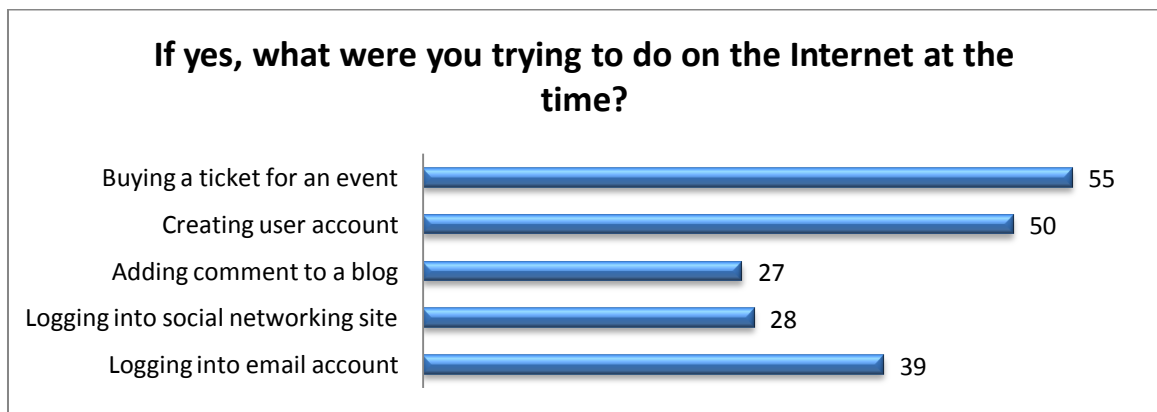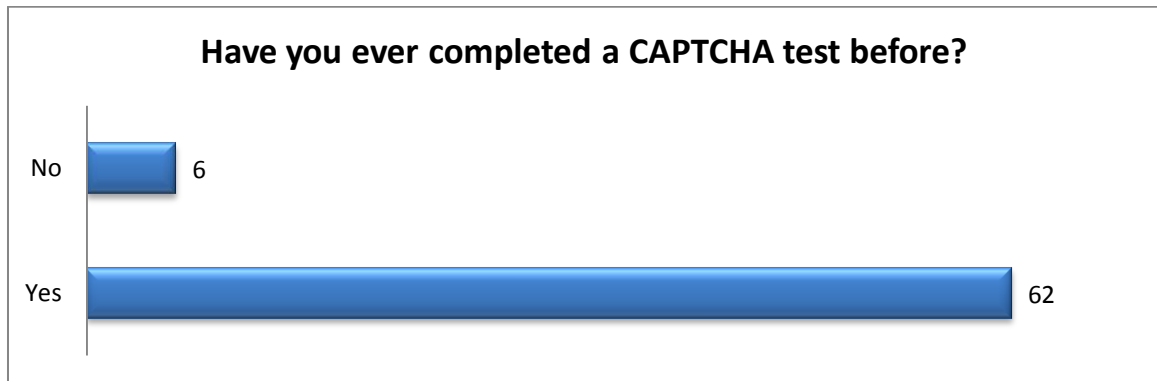
**<u>Other</u>**

"Get a quote for transport of goods"

"Submitting a post to 4chan.org. Which is not a site I would recommend that anyone visit, ever."

"airline ticket"

"cases where I've mistyped my password"

"Downloading files from mega upload, similar file sharing sites. Also Ryanair."


**<u>Any Comments relating to your experience of completing a CAPTCHA?</u>**

Case sensitivity and character recognition can be cumbersome

Pain, as they are difficult to get right.

Frustrating, sometimes hard to make out the letters.

So annoying. Don't like them at all. I very often get them wrong

It is crap. I can never type the correct thing

They're the best mechanism I have yet seen to ensure the page is being viewed by a human.

They can be very hard to read. It can take up to 3 attempts to get it correct.

They are a useful means of preventing robots overwhelming websites, but they can be annoying, particularly when they have been poorly composed.

I get it wrong about 25% of the time now

Bloody annoying, especially when I can't read the feckin letters, or if I am using my phone it is so hard to read.

Had trouble on occasion with the perceptual recognition of letters due to their disortion, particularly if there is pattern as the background

They can be confusing

Some are reasonably straightforward but the spaces between distorted letters and the presence or absence of serifs often mean that identification of the characters is needlessly difficult.

They do my nut in! I'm not great at seeing hidden or distorted shapes/letters/numbers

They are a pain in the ass. Usually, they are too long.

Sometimes can be hard to make out.

Sometimes it's hard to determine what the letters are.

Sometimes It's hard to see the letters clearly.

Don't like them

It's a pain in the ass dude!

Not usually a problem. And I don't mind when it is a "reCAPTCHA" as I know this is helping to proofread old books for everyone's benefit.

nope !

they suck

About half of them aren't actually readable!

Generally I require at least one refresh before I can successfully complete it. They are annoying and occasionally have discouraged me from proceeding

no

i sometimes get it wrong. when this happens and it makes me fill in information on the form again like password etc i get very frustrated.

Most of the time I can't read the content and very often have to request a new picture.

I hate CAPTCHA, they're an inconvenience for users and there is tons of programs and scripts out there that web trawlers use to automatically skip them, essentially making them useless as they're supposed to prove it's a human trying to access the content

They are a nightmare to use, can't imagine how anyone with sight issues can use them.

Recaptcha is used to index words that were not automatically recognised using OCR tech. Good idea. Only one of the words, usually the most legible of the two is required.

Few CAPTCHA's are very easy for me to figure out but very rare the cursive effect exhibit hard to figure out .As I have observed in few online website they provide a button when clicked displays the different CAPTCH picture but few don't provide this button which hence when done with the guesswork,the form will be submitted and the error will be displayed by reseting fields.

CAPTCHA is more or less pointless, and can be defeated by automated means.

Sometimes with ReCAPTCHA I try to take shortcuts and guess which word is being validated. I am aware this is wrong and defeats the point of it. But its nice to beat the system now and again :)

Gets confusing most of the times!

Sometime the distortion is too much, making it too hard to read. Thank god for the refresh button.

When you can't read then, the reading/sounding technology usually requires and install, its just too much hassle!

CAPTCHA generated images are often unintelligible, using random cutouts or badly scanned images and often feel cumbersome in there use. Another, more intuitive security measure would be a welcome change

Sometimes the distorted letters can be unreasonably difficult to identify and it takes 2 or 3 goes to get it right.

slow, therefore annoying

They seem to be getting more and more difficult to decode, typically it now takes me several attempts to get past it.

I find on some sites the letters are unreadable.

Never get the letters right the first time. Have to try a couple of times

## APPENDIX F: INTERVIEW TRANSCRIPTS

<u>**Male 66yrs**</u>

| | |
|---|---|
| **Interviewer:** | Do you own a desktop computer? |
| **Respondent:** | Yeah, an ordinary computer yes. |
| **Interviewer:** | Do you own a laptop? |
| **Respondent:** | No. I own an iPhone |
| **Interviewer:** | Ok so you own a smart phone. Do you own an iPod? |
| **Respondent:** | No I don't. |
| **Interviewer:** | Is there a webcam on your desktop? |
| **Respondent:** | Yes with a microphone. |
| **Interviewer**: | Ok cool and do you own a tablet, like an iPod or anything like that? |
| **Respondent:** | No |
| **Interviewer:** | How many hours a week do you think you'd normally spend using any of the electronic devices that you own? |
| **Respondent:** | eh.... |
| **Interviewer:** | So whether it's your computer or your phone? |
| **Respondent:** | I'd say around 5... 6 hours |
| **Interviewer:** | A week? |
| **Respondent:** | Yeah |
| **Interviewer:** | Ok. So when it comes to using a computer, have you have read sent or wrote an email? |
| **Respondent:** | oh yes yes. |
| **Interviewer:** | Have you read, wrote a document in word? |
| **Respondent:** | yeah. |
| **Interviewer:** | Have you created a macro in Excel? |
| **Respondent:** | I don't know. I don't know what that is. |
| **Interviewer:** | You know when you create rules and stuff, so that if you fill in a value into a certain cell, you can add logic to manipulate that data |
| **Respondent:** | Oh yeah, no I haven't. I don't do that. |
| **Interviewer:** | Have you create a presentation in PowerPoint? |

| | |
|---|---|
| **Respondent:** | No |
| **Interviewer:** | Have you ever played computer games? |
| **Respondent:** | Yes |
| **Interviewer:** | Have you ever downloaded or listened to music? |
| **Respondent:** | Yes |
| **Interviewer:** | Have you ever surfed the Internet? |
| **Respondent:** | Yes |
| **Interviewer:** | Have you ever bought an item online? |
| **Respondent:** | Not directly. I normally get others to do it for me. |
| **Interviewer:** | And have you ever created a website or developed any computer software? |
| **Respondent:** | Oh I have bought online. I've bought airline tickets. |
| **Interviewer:** | Oh ok cool. And have you ever developed a website or any software? |
| **Respondent:** | No no I haven't |
| **Interviewer:** | So in terms of, there's a few different issues I have here with regards with IT. So you just need to tell me if it is something that you would ever think about, or be concerned about, right? So the age of your computer or your computer software? |
| **Respondent:** | eh yeah an old computer that's slow bothers me |
| **Interviewer:** | ok so, slow internet access? |
| **Respondent:** | yeah that bothers me |
| **Interviewer:** | do you ever worry about the skill level you have trying to troubleshoot a problem that you might have on your computer? |
| **Respondent:** | yeah |
| **Interviewer:** | so you ever worry about computer virus? |
| **Respondent:** | oh yes all the time! |
| **Interviewer:** | ok, spam? |
| **Respondent:** | the computer deletes it now automatically thank god so I don't worry about it |
| **Interviewer:** | any else then with computers that bothers you, concerns you or annoys you in general that you can think of? |

| | |
|---|---|
| **Respondent:** | no I find them very convenient and I find the fact that you can file letters on your computer under all the various headings very useful. It's like a filing cabinet. |
| **Interviewer:** | yeah there's definitely a lot of pros to using computers anyway |
| **Respondent:** | oh definitely |
| **Interviewer:** | erm, ok, so, I want to talk about CAPTCHA now. |
| **Respondent:** | What? |
| **Interviewer:** | I'll explain what that is now. You know sometimes when you are on a website, and it shows you a bunch of letters that you have to type out... actually you know I can show you a picture. |
| **Respondent:** | oh you know what, yeah I know what you are talking about. I know what it is... |
| **Interviewer:** | let me just show you an image here.... see here |
| **Respondent:** | oh yes Ryanair has them. I really hate them you know |
| **Interviewer:** | ok, so you've had to use them before then? |
| **Respondent:** | yes many times yes. |
| **Interviewer:** | ok, and from buying something online. Have you ever seen it when logging into your email, or on a blog or something, maybe even creating an account for something, have you ever seen it there? |
| **Respondent:** | I don't know, I just know I've seen it on Ryanair. All the airlines have it actually before you can look up process properly so it's difficult |
| **Interviewer:** | so how do you feel about them? |
| **Respondent:** | Don't like them at all, because I very often get them wrong |
| **Interviewer:** | ok so in terms of getting around CAPTCHA, it is possible that instead of having to use this type of security test to show that we are a human being to the computer in different ways. We could use different forms of identification. So maybe you could use your fingerprint, or face recognition.. |
| **Respondent:** | oh yeah yeah |
| **Interviewer:** | something that shows you are human, that a computer couldn't fake. Ok so with this idea, different online site could ask for this biometric information. Like Google could ask you to scan in |

153

|  |  |
|---|---|
|  | your fingerprint when you are logging into Gmail, or the government could ask for your fingerprint if you were logging in online to an account where maybe you could pay for your bin tags or check you tax information but with this these organisations would have to store some of this information on their databases... |
| **Respondent:** | ok... |
| **Interviewer:** | so would you allow Google to store your fingerprint information if it meant that your account would be hacked |
| **Respondent:** | yeah i think so |
| **Interviewer:** | and would you be happy with the government having the same information. |
| **Respondent:** | no |
| **Interviewer:** | what if it meant that you didn't have to type in your username and password and so was quicker to sign in, would you be happy with the government having the information then? |
| **Respondent:** | hmm yeah maybe.... I'd prefer the fingerprint to be on my own computer, then on theirs |
| **Interviewer:** | absolutely, but in this case in order for the mechanism to work, your fingerprint would have to be on their computer... |
| **Respondent:** | it would be? hmm... |
| **Interviewer:** | so would you still be happy then with Google having your fingerprint information? Like so instead of typing in your username and password, you could simply scan your finger... |
| **Respondent:** | I think I'd prefer actually to type it in. |
| **Interviewer:** | Ok and with the government? |
| **Respondent:** | oh I'd prefer to definitely type it in with the government. I would trust Google more than the government |
| **Interviewer:** | ok, why would you trust Google more than the government? |
| **Respondent:** | because, I think Google is a commercial organisation who do things for profit. The government tend more often to just be corrupt for the sake of being corrupt, or cover up. They are more dishonest |

| | |
|---|---|
| **Interviewer:** | ok, so but what if it meant that by the government having this information it would mean that you didn't need to use CAPTCHA? |
| **Respondent:** | No I don't want them to have my fingerprint information ever. For anything |
| **Interviewer:** | and with Google? Would you be happy for them to store your fingerprint if it meant that you didn't need to use CAPTCHA on their site? |
| **Respondent:** | oh yeah I'd be happy for Google to have it to get away from CAPTCHA |
| **Interviewer:** | ok what if then Google made a new rule, which meant you had to give them your fingerprint in order to have a Gmail account? |
| **Respondent:** | no I wouldn't be happy if it was mandatory. |
| **Interviewer:** | and the government? |
| **Respondent:** | no |
| **Interviewer:** | have you ever had to scan in your fingerprint? |
| **Respondent:** | no I don't think so. |
| **Interviewer:** | have you ever been to the states? |
| **Respondent:** | yeah |
| **Interviewer:** | did you have to give in your fingerprint when going through immigration? |
| **Respondent:** | no, don't think so. Would I have had to? |
| **Interviewer:** | I mean I know you have to now. When were you last in the states? |
| **Respondent:** | for the world cup, so in 1994. |
| **Interviewer:** | Yeah I don't know if you had to give it in then, all I know is you have to give it in now. |
| **Respondent:** | well I don't think I did.... or maybe I did... I don't remember |
| **Interviewer:** | But if you were going to the states now, would you give them your fingerprint? |
| **Respondent:** | yeah id with that |
| **Interviewer:** | so what makes that different then from giving your fingerprint for these online accounts? |

| | |
|---|---|
| **Respondent:** | because I think that's in a particular location. You know it's not in a boarder area like on the Internet. I would at least now then what department my information is being stored in. or at least I would hope that they don't spread it around. Although I suppose I don't know if they do or not. I mean that's a security set up that we just have to tolerate. Like I want to go to the states, so I know I have to give in my fingerprint. But I could live without the online account |
| **Interviewer:** | what if the government promised that they would keep you fingerprint information purely for the online account and no spread it around and use it elsewhere? |
| **Respondent:** | no I just wouldn't trust them. |
| **Interviewer:** | ok so that's your fingerprint, but there are other ways to identify yourself using other means. Like voice recognition.  Would you be happy for Google to store a sample of your voice on their databases? |
| **Respondent:** | yeah id be happy with that |
| **Interviewer:** information? | and would you be happy for the government to have that |
| **Respondent:** | no no. I think government information gets abused. |
| **Interviewer:** | ok, but what if you could talk into a microphone and be logged into your government online account without having to type anything, or use a CAPTCHA? |
| **Respondent:** | No not the government, but with Google id be happy |
| **Interviewer:** | ok, I'm seeing a trend here. |
| **Respondent:** | yeah, ha ha ha, it is a trend |
| **Interviewer:** | ok so we also have facial recognition. Would you be happy for Google to have a picture of your face in their databases? |
| **Respondent:** | no I don't think so. No |
| **Interviewer:** | and the government? |
| **Respondent:** | no... Well the government do already I suppose. They have my face. But its under a particular.... i have to give it to get a passport. But it's not used in other circumstances. |

156

| | |
|---|---|
| **Interviewer:** | so you be happy for the government to have a picture of you face to help you log into your online account? |
| **Respondent:** | no, not for the purposes of logging into my account. For my passport its fine |
| **Interviewer:** | but you know if they had this information it would mean that you would have to type in your username, or use CAPTCHA? |
| **Respondent:** | no I don't really want anyone having my photograph |
| **Interviewer:** | ok, that's fine. Ok so then your iris. You can scan you iris to uniquely identify yourself cos everyone has a very unique iris. Would you be happy for Google to have this information? |
| **Respondent:** | yeah yeah now I would prefer that. |
| **Interviewer:** | so you'd be happy for Google to have that? |
| **Respondent:** | yeah. And I think I would probably allow the government to have that information. |
| **Interviewer:** fingerprint? | ok. Why so why are you happy with the iris and not the |
| **Respondent:** | I just think it would be less easy to abuse... or at least that's what I would have thought |
| **Interviewer:** | why do you think that? |
| **Respondent:** | I don't know. I just think it would be harder to identify me using an iris scan. Like, it's not something I scan often. Whereas I'm probably leaving fingerprints all over the place and I certainly talk about. But if the iris information was abused, or cropped up somewhere it shouldn't I would know immediately that, oh Google are abusing that information, or the government are abusing it |
| **Interviewer:** | ok, yeah, that makes sense. |
| **Respondent:** | are you just saying that to me? |
| **Interviewer:** | no, no, it does make sense definitely. Scanning your iris is definitely not something you do as part of your everyday. |
| **Respondent:** | yeah exactly |
| **Interviewer:** | ok so last one then... you could use your handwriting to identify yourself. Would you be happy with Google having this information? |

| | |
|---|---|
| **Respondent:** | no |
| **Interviewer:** | and the government? |
| **Respondent:** | no not in those circumstances. No when it's all done over the Internet. Now I know that the government already have my signature but... I feel that's different. It might depend on the amount of a sample they wanted. Like maybe I'd give in my signature. But maybe not a whole paragraph or writing. You know? |
| **Interviewer:** | Yeah absolutely. Well that's it |
| **Respondent:** | all done? |
| **Interviewer:** | all done. Thanks very much. |
| **Respondent:** | no problem. |

**Female – 64**

| | |
|---|---|
| **Interviewer:** | which of the following electronic devices do you own? I'm going to list a few and you just let me know |
| **Respondent:** | ok |
| **Interviewer:** | desktop computer? |
| **Respondent:** | what's that? |
| **Interviewer:** | just a normal computer |
| **Respondent:** | oh yes I do |
| **Interviewer:** | a laptop computer |
| **Respondent:** | no |
| **Interviewer:** | iPad |
| **Respondent:** | no |
| **Interviewer:** | a smart phone |
| **Respondent:** | is that different than a normal phone? |
| **Interviewer:** | it's a little different. Show me the phone you have |
| **Respondent:** | this one [shows phone] |
| **Interviewer:** | ok that's just a normal cell phone. A music device, like an iPad |
| **Respondent:** | I have a radio? |
| **Interviewer:** | no that's a little different. I'll mark it down as no |
| **Respondent:** | ok |
| **Interviewer:** | a webcam? |

| | |
|---|---|
| **Respondent:** | no |
| **Interviewer:** | a microphone? |
| **Respondent:** | no |
| **Interviewer:** | do you ever use Skype? |
| **Respondent:** | oh yes. |
| **Interviewer:** | and when you are using Skype can the person see and hear you? |
| **Respondent:** | yes.... oh... oh I do have a webcam with a microphone built in |
| **Interviewer:** | ok. How many hours a week do you spend on these electronic devices a week? |
| **Respondent:** | erm... I would say a half an hour a week |
| **Interviewer:** | ok. I'm going to list a few activities to you and you tell me if you have ever done them on a computer |
| **Respondent:** | ok |
| **Interviewer:** | ok, using email? |
| **Respondent:** | yes |
| **Interviewer:** | have you ever read or wrote a document in word |
| **Respondent:** | no |
| **Interviewer:** | have you ever written a macro in excel |
| **Respondent:** | I don't even know what that means |
| **Interviewer:** | ok. Have you ever played a computer game? |
| **Respondent:** | eh... yes... Tetris |
| **Interviewer:** | have you ever downloaded or listened to music on a computer? |
| **Respondent:** | no |
| **Interviewer:** | have you ever surfed the Internet |
| **Respondent:** | no... Oh I mean... is that just looking at different sites? |
| **Interviewer:** | yes |
| **Respondent:** | oh yeah I've done that |
| **Interviewer:** | have you ever shopped online? |
| **Respondent:** | no. I just get other people do to that for me. I wouldn't have a clue |
| **Interviewer:** | ok so it's safe to say you haven't developed a website or computer software |
| **Respondent:** | ehhhh... ha... no. Basically you can put me down for no on everything |

| | |
|---|---|
| **Interviewer:** | is there anything when it comes to computers and technology that concerns you? |
| **Respondent:** | not really. I can't think of anything |
| **Interviewer:** | ok ill list a few hear and you tell me if you can relate to it |
| **Respondent:** | ok |
| **Interviewer:** | do you ever get worried about the age of your computer? Like how old it is? |
| **Respondent:** | no |
| **Interviewer:** | do you ever get worried about slow internet access |
| **Respondent:** | no |
| **Interviewer:** | do you ever get worried about your skill level in troubleshooting problems with your computer? |
| **Respondent:** | I don't worry about it. |
| **Interviewer:** | ok maybe worry is a strong word, but do you ever get concerned about it, or think about it? |
| **Respondent:** | yeah... well... id probably prefer to be better at computer. But I'm not losing sleep over it |
| **Interviewer:** | are you ever concerned about computer viruses? |
| **Respondent:** | no. I just get other people to fix that stuff for me |
| **Interviewer:** | are you concerned about spam |
| **Respondent:** | no I wouldn't even know what spam is ha ha ha |
| **Interviewer:** computers? | so there's nothing really at all that worries you about |
| **Respondent:** | ha ha, as my family say, I don't worry about anything. I think everything is brilliant |
| **Interviewer:** | have you ever seen anything like this before [shows a picture of CAPTCHA] |
| **Respondent:** | that's those arith-magrams, or whatever you call them. |
| **Interviewer:** | they're called CAPTCHA. |
| **Respondent:** | oh yeah. I remember trying to read them. They're the things I tested before with you |
| **Interviewer:** | yeah. Have you used them before on a computer? |
| **Respondent:** | yeah with you. |
| **Interviewer:** | but without me? |

160

| | |
|---|---|
| **Respondent:** | no. never used them before that |
| **Interviewer:** | and in that test, what did you think of them? |
| **Respondent:** | I don't know what they're for |
| **Interviewer:** | how was your experience? Did you find them easy to do? |
| **Respondent:** | well I read a few of them and thought they were ok |
| **Interviewer:** | ok so I'm going to give you two scenarios now. Because instead of using those tests, maybe one day in the future websites could ask you to give in your fingerprint or do face recognition in order to allow you to log into your like Gmail account, or maybe pay for you bin tags online. This could be used instead of CAPTCHA, cos although you have no problem with them, some people with disabilities find it difficult to use. But with this some of these organisations like Google and the Government would have to store your fingerprint or face information on their computers. |
| **Respondent:** | ok |
| **Interviewer:** | ok so would you be happy for Google to store your fingerprint information on their own computers? |
| **Respondent:** | yeah |
| **Interviewer:** information? | ok would you be happy with the government having this |
| **Respondent:** thing. | eh don't know. In a way I'd be afraid of a big brother type of |
| **Interviewer:** | with the government? |
| **Respondent:** | yeah.... well it's a concern.... no I don't think I'd be happy with the government having that information. |
| **Interviewer:** | but you'd be happy with Google? |
| **Respondent:** | eh... no I don't think so. I changed my mind |
| **Interviewer:** | ok why? |
| **Respondent:** | because of a security thing. You know, could be used against you. Maybe not this year, or next year, maybe 20 years down the road. Maybe you could be blamed for a crime that you didn't commit |

| | |
|---|---|
| **Interviewer:** | ok yeah that makes sense. Have you ever used a fingerprint scanner before? Or had to use ink to take a fingerprint? |
| **Respondent:** | no |
| **Interviewer:** | would you be happy for Google to store a sample of your voice? |
| **Respondent:** | I don't know. No. see? I don't know. |
| **Interviewer:** | what's your hesitation? |
| **Respondent:** | I don't know. Same thing again really. I wouldn't be as against the voice as the fingerprint? |
| **Interviewer:** | why is that? |
| **Respondent:** | cos the fingerprint is your fingerprint. You could change your voice. But you can't change your fingerprint. |
| **Interviewer:** | ok. Would you be happy for the government to have a sample of your voice? |
| **Respondent:** | yeah I wouldn't be as opposed to that. |
| **Interviewer:** | so you'd be happy with the government and Google having this information or not? |
| **Respondent:** | happyish for both. |
| **Interviewer:** | ok would you be happy for Google to store a picture of your face? So they could do facial recognition. |
| **Respondent:** there. | see it's another big brother thing. Too much information out |
| **Interviewer:** | would that be a concern you have with technology in general? |
| **Respondent:** | what? |
| **Interviewer:** | that there's too much information out there? |
| **Respondent:** | ok yes, definitely. All the kids now, putting all there information on that Facebook. I just don't agree with it |
| **Interviewer:** | so would you be happy for Google to have this information of your face? |
| **Respondent:** | no |
| **Interviewer:** | and the government? |
| **Respondent:** | well... yeah id be ok with that. They probably be ok with that. Cos sure my picture is on my driver's license so. Actually you know I think I'd be happy for Google to have that information too. |

| | |
|---|---|
| **Interviewer:** | what has made you change your mind? |
| **Respondent:** | I sort of feel that a picture of your face wouldn't be as bad as a fingerprint |
| **Interviewer:** | why? |
| **Respondent:** | well you could dye your hair or get plastic surgery to change your nose. But you can't change your fingerprint. |
| **Interviewer:** | ok. Another way of identifying yourself is by scanning in a picture of your iris |
| **Respondent:** | how do they do that? |
| **Interviewer:** | [demonstrate how a user would press their eye up to an iris scanner device] they'd just go like this. And then an infrared light scans you iris structure |
| **Respondent:** | oh right. And that's like a fingerprint? |
| **Interviewer:** | yeah it would uniquely identify you like a fingerprint. So would you be happy with the government storing this type of information? |
| **Respondent:** | yeah |
| **Interviewer:** | and Google? |
| **Respondent:** | yeah |
| **Interviewer:** | so why are you ok with the iris but not the fingerprint with Google? |
| **Respondent:** | well I just feel that... well I don't know really... I never knew you could take a picture of your iris... is it ok to say I don't know? |
| **Interviewer:** | yeah that's fine. Would you be happy for Google to have a sample of your handwriting? |
| **Respondent:** | no. |
| **Interviewer:** | even if that meant it would make your Gmail account more secure and you didn't have to type in your username or password? |
| **Respondent:** | oh well, yeah I suppose I'd be happy then |
| **Interviewer:** | would you be happy for the government to have this information |
| **Respondent:** | yeah |
| **Interviewer:** | and why are you happy with this? |

| | |
|---|---|
| **Respondent:** | well handwriting is not really a big deal. Sure I've been signing my life away for years. I'm sure companies all over Ireland have a sample of my handwriting |
| **Interviewer:** | Have you ever had to write something electronically, you know, using a stylus or something? |
| **Respondent:** | oh yeah, signing for a thing that came in the post. |
| **Interviewer:** | ok. And you were ok with using that? |
| **Respondent:** | yeah |
| **Interviewer:** | ok cool. That's it. Thanks |
| **Respondent:** | that's it? Great. |

**Male - 40**

| | |
|---|---|
| **Interviewer:** | ok which of the following electronic devices do you own? A desktop computer? |
| **Respondent:** | in work yeah |
| **Interviewer:** | a laptop? |
| **Respondent:** | my wife officially owns it, but I use it most of the time |
| **Interviewer:** | a tablet? |
| **Respondent:** | yeah |
| **Interviewer:** | a smart phone? |
| **Respondent:** | yes |
| **Interviewer:** | a music devices? |
| **Respondent:** | no. well on my smart phone I keep my music |
| **Interviewer:** | webcam? |
| **Respondent:** | no |
| **Interviewer:** | microphone? |
| **Respondent:** | no |
| **Interviewer:** | have you ever skyped before? |
| **Respondent:** | yeah all the time... oh I have a webcam and microphone built into my iPad |
| **Interviewer:** | oh ok cool. How many hours a week would you say you spend using those electronic devices? |
| **Respondent:** | that's an interesting question. Does that include work? |
| **Interviewer:** | yeah |

| | |
|---|---|
| **Respondent:** | eh.... so in work about 5 hours a day, 5 times a week. So that's 25. And I'd normally spend about an hour when I get home each day, so that another 5 hours, plus I probably go on the laptop during the weekend, so... |
| **Interviewer:** | ok so you'd probably spend over 30 hours a week... |
| **Respondent:** | yeah definitely. |
| **Interviewer:** | which of the following activities have you performed on a computer, use email? |
| **Respondent:** | yes |
| **Interviewer:** | read or wrote a document in word? |
| **Respondent:** | yeah |
| **Interviewer:** | wrote a macro for excel? |
| **Respondent:** | I don't know what a macro is. |
| **Interviewer:** | So you can add rules for each cell, to manipulate the data? |
| **Respondent:** | oh like a spreadsheet? |
| **Interviewer:** | yeah, have you done that before? |
| **Respondent:** | yeah |
| **Interviewer:** | have you ever created a PowerPoint presentation? |
| **Respondent:** | no |
| **Interviewer:** | ever played computer games |
| **Respondent:** | yes only silly ones on my phone |
| **Interviewer:** | download or listening to music |
| **Respondent:** | no not really |
| **Interviewer:** | have you never done that before, no? |
| **Respondent:** | yeah I have, but not much |
| **Interviewer:** | have you ever shopped online? |
| **Respondent:** | bought books online |
| **Interviewer:** | did you ever create a website? |
| **Respondent:** | no. well I did one once for a football team I was on, on one of those free sites. But it was pretty crap |
| **Interviewer:** | have you ever developed computer software? |
| **Respondent:** | no |
| **Interviewer:** | anything in particular when it comes to it, technology or the Internet that concerns you |

| | |
|---|---|
| **Respondent:** | privacy issue. I think you're giving a lot of information into the public domain. And you may not be aware that you're putting it out there and you may not want it to be there, but you are. In years to come you might wish you didn't put the information out there |
| **Interviewer:** | and have you ever had that experience before? |
| **Respondent:** | no really? I try not to put that type of information out there? |
| **Interviewer:** | do you own a Facebook account? |
| **Respondent:** | I do |
| **Interviewer:** | and do you put any information up on that? |
| **Respondent:** | I do, but not much. I literally have like 2 photos on it and I never update it |
| **Interviewer:** | ok. Would you be concerned about the age of you computer? |
| **Respondent:** | yes |
| **Interviewer:** | would you be worried about slow internet access |
| **Respondent:** | yes |
| **Interviewer:** | would you ever be concerned about your technical skill? |
| **Respondent:** | yes. That's a yes in bold capitals |
| **Interviewer:** | ha ok. Ever worried about computer virus and spam? |
| **Respondent:** | yes |
| **Interviewer:** | anything else you want to add? |
| **Respondent:** | about concerns with it? |
| **Interviewer:** | yeah. |
| **Respondent:** | no I think you have pretty much covered |
| **Interviewer:** | ok so have you ever completed a CAPTCHA before? |
| **Respondent:** | eh... can I go back there again, about the concerns? |
| **Interviewer:** | yeah. |
| **Respondent:** | sometimes I think you can spend your whole life on the Internet. It's not all that interesting. In work I've had to make a conscience effort to stay away from the Internet. You know? It's no very productive. Going out to the same sites out of habit to see if there are any new updates, and you realise it's a huge waste of time. And I would be concerned from my point of view and society's point of view, that everyone is spending their life |

|  |  |
|---|---|
|  | in the internet, without actually getting up, going outside and doing something. So I've had a to make a conscience effort not to comment on those sites and not to read them too much. Maybe just read them once a day. |
| **Interviewer:** | so do you hope in the future you would not have to spend so much time in front of the computer? |
| **Respondent:** | yeah, I'd like to have it more structured, and a better balance |
| **Interviewer:** | ok |
| **Respondent:** | id just be concerned you know, like Facebook, I think since Christmas I've only gone on a couple of times. I found myself going on to read people's silly comments and to look at their random photos, and you know, it's just silly stuff. Just had to say, right I'm spending my life on this site, and I cut it out. And it was easier than I thought it was going to me |
| **Interviewer:** | ok cool. Happy to move on? |
| **Respondent:** | yeah... |
| **Interviewer:** | fell better after that? |
| **Respondent:** | yeah I do. |
| **Interviewer:** | ok have you ever used CAPTCHA before |
| **Respondent:** | yes |
| **Interviewer:** | when have you seen it? |
| **Respondent:** | buying tickets on Ticketmaster, and logging in to stuff |
| **Interviewer:** | Ok and how do you feel about CAPTCHA |
| **Respondent:** | I don't really like it. I seem to get it wrong a bit |
| **Interviewer:** | and if there was a way to get around CAPTCHA but still get the benefits of CAPTCHA would you go for it? |
| **Respondent:** | yeah definitely. |
| **Interviewer:** | ok so moving on. I'm going to give you two scenarios... ok? |
| **Respondent:** | ok |
| **Interviewer:** | so instead of using CAPTCHA to tell a computer that you are a human, you could do that in a different way. You could use a scan of your fingerprint or face recognition to show that you weren't a robot. But with this, you'd have to let the website organisation store your information. Like Google for example, |

|  |  |
|---|---|
|  | you could log into your Gmail account using your fingerprint, or like to get into an online account where you could see your tax information. So would you be happy for Google to store you fingerprint information? |
| **Respondent:** | I don't think so no. |
| **Interviewer:** | even if it meant that it would prevent your account being hacked? |
| **Respondent:** | no |
| **Interviewer:** | why not? |
| **Respondent:** | I think your fingerprint is very unique to you. And it would be very difficult to deny you're fingerprint. Well, it would be impossible to deny it. And you'd find that Google would build up a pretty interesting profile about you. They'd know your personal and private information. So no I wouldn't be keen on them having my fingerprint. |
| **Interviewer:** | Would you be happy for the government to have this information? |
| **Respondent:** | no. same. Again, the government you can trust 90% of them, but it's the 10% that could get you into trouble |
| **Interviewer:** | so let's say then Google said you are not allowed have a Gmail account unless you give us your fingerprint. Would that change your mind? |
| **Respondent:** | no I don't think so. |
| **Interviewer:** | if the government said the same? |
| **Respondent:** | no in fact that would make me feel even stronger about it. Because you're not even required to carry identification with you, so why would they all of a sudden want your fingerprint, then no. And if it meant sacrificing the benefits of these websites, I still say no. |
| **Interviewer:** | have you ever used a fingerprint scanning device? |
| **Respondent:** | no |
| **Interviewer:** | so the new passports coming out might have some biometric information on them. How do you feel about that? |

| | |
|---|---|
| **Respondent:** | well I'm not sure if I'd be happy about it. But for a passport, like I want a passport. So if that's what I have to so then that's what I have to do. Like if it was the law to give it, then I wouldn't really have a choice. |
| **Interviewer:** | if the government or Google swore that they wouldn't use the information incorrectly, would that change your mind? |
| **Respondent:** | no no. I don't trust them. It means nothing. No even scouts honour. |
| **Interviewer:** | ha yeah absolutely. Ok. So then another way to identify you would be to use your voice. So in the same way, would you be happy for Google to have this information and to store it? |
| **Respondent:** | yeah, I don't feel that wouldn't be as bad. Not as bad as the fingerprint. |
| **Interviewer:** | and why do you think that? |
| **Respondent:** | well like you could refuse to talk or change your voice if someone was trying to prosecute you. So I think I'd be ok with the voice. Like if I could log into Gmail using your voice to say your username, I think that would be pretty handy. I'd like that |
| **Interviewer:** | and what about the government? |
| **Respondent:** | I feel the same. Its kind of the same as a signature isn't it? Like I'd like to know what it was being used for. But I think I'd be ok with it. |
| **Interviewer:** | ok so another way to log in could be to use face recognition. So would you be ok with Google storing a picture of your face on their database? |
| **Respondent:** | eh I don't know. I'd be reluctant. |
| **Interviewer:** | what's the reluctance? |
| **Respondent:** | same as fingerprint. Your face would be the same as your fingerprint. It's something that you can change. I suppose your fingerprint and your face could be analysed unknownst to you. Like you could be going to a football match or a political rally and someone could be collecting all this data about your whereabouts. No. I wouldn't be too keen on that. I can see advantages to it though. You know, like I've a diary with all my |

169

passwords cos I can never remember them. And if I could just sit in front of my webcam and be given access to my Gmail account. I think that would be great. But I prefer not to use my face information. Maybe something else, but not with my face.

**Interviewer:** would you be happy with the government having your face information?

**Respondent:** no, same thing. Wouldn't be happy with it.

**Interviewer:** do you have a passport?

**Respondent:** yeah, yeah I know they have my passport but like I presume they don't have it digitally captured. Like it just on a piece of paper somewhere in the passport office.

**Interviewer:** ok.

**Respondent:** you're just agreeing with me, I'm probably all over the place here.

**Interviewer:** no no I think you're making sense. Would you put a picture of yourself on Facebook?

**Respondent:** eh... like i have one for my intro. But I think that's it. Me and a statue of a dinosaur. I put the dinosaur there to throw them.

**Interviewer:** ha ha. Good thinking! Ok so another way of identifying yourself is using an iris scan. Would you be happy with giving Google your iris information?

**Respondent:** I don't know. See all these questions you ask... like the most important information is my bank details. And I'm happy to go online and do my banking that way. But if you went to my equivalent 30 years ago and told them they'd be banking online, they would have been totally against it. You know? They would have thought it was totally insecure. But nowadays we all do it and we have no problem with it. so I'm wondering am I saying no to all these face recognition and iris recognition, but in reality in a couple of years I'd be happy to give that information in. even just because other people are using the same service and are giving in their face information and such. I'd probably just follow along. So maybe I'd be ok with the iris scanning. And if

| | |
|---|---|
| | this technology existed and worked, the advantages would fair out weight the negatives. |
| **Interviewer:** | so why are you ok with the iris, but not the face or fingerprint? |
| **Respondent:** | well I presume the only way they can get an iris scan is by putting your eye up to a proper scanner. |
| **Interviewer:** | yeah |
| **Respondent:** | like they can't take a picture of me and get my iris information? |
| **Interviewer:** | no. you need to use a proper scanner, because it actually takes a scan of the blood vessels in your eyeball. |
| **Respondent:** | ok. Cos id be afraid with face and fingerprint that someone would be compiling my data and information behind my back. Like taking pictures of me and taking my fingerprints off stuff I own and collecting all this data. At least with the iris, they wouldn't be able to do that. I'd have to use this scanner to give in the information. I couldn't give that information away by accident. Still same again, my concerns with any of this, I might just get over it and in 10 years I'll be happy to give this information ok. |
| **Interviewer:** | ok so last one then, would you give Google a sample of your handwriting. And this would be a way to uniquely identify you. |
| **Respondent:** | yeah I think handwriting or like a signature id be ok with. Like that information is already out there. |
| **Interviewer:** | and the government? |
| **Respondent:** | again, it's already out there. So I'd be ok with that. |
| **Interviewer:** | ok perfect. That's it. That's for doing the interview |
| **Respondent:** | no problem |

**Male - 37**

| | |
|---|---|
| **Interviewer:** | which of the following devices do you own? |
| **Respondent:** | ok |
| **Interviewer:** | desktop? |
| **Respondent:** | yes |

| | |
|---|---|
| **Interviewer:** | a laptop? |
| **Respondent:** | yes |
| **Interviewer:** | a tablet? |
| **Respondent:** | yes |
| **Interviewer:** | a smart phone? |
| **Respondent:** | yes |
| **Interviewer:** | a webcam, even if it's integrated in your laptop or something? |
| **Respondent:** | yes |
| **Interviewer:** | a microphone? |
| **Respondent:** | yes, that's built into my webcam |
| **Interviewer:** | ok. How many hours a week do you spend using these electronic devices? |
| **Respondent:** | including work? |
| **Interviewer:** | yeah |
| **Respondent:** | probably about... eh.... about 28-30 hours I think |
| **Interviewer:** | ok so I just want to get an idea of stuff that you might have done on a computer for. |
| **Respondent:** | ok |
| **Interviewer:** | using email |
| **Respondent:** | yes |
| **Interviewer:** | using Microsoft word |
| **Respondent:** | yes |
| **Interviewer:** | creating a macro in excel |
| **Respondent:** | yes |
| **Interviewer:** | creating a PowerPoint presentation |
| **Respondent:** | yes |
| **Interviewer:** | playing computer games |
| **Respondent:** | yes |
| **Interviewer:** | downloading or listening to music |
| **Respondent:** | yes |
| **Interviewer:** | surfing the internet |
| **Respondent:** | yes |
| **Interviewer:** | shopping online |
| **Respondent:** | yes |

| | |
|---|---|
| **Interviewer:** | developing a website |
| **Respondent:** | yes |
| **Interviewer:** | developing computer software |
| **Respondent:** | well... a long time ago, but yes |
| **Interviewer:** | ok so is there anything when it comes to computers or it that concerns you? |
| **Respondent:** | concerns me? |
| **Interviewer:** | yes |
| **Respondent:** | erm... no |
| **Interviewer:** | ok I have a list here I want to run by you to see if you can relate to them. Are you concerned about the age of your computer or the software on it? |
| **Respondent:** | no |
| **Interviewer:** | concerned about slow internet access? |
| **Respondent:** | concerned, as in it causes me concern? |
| **Interviewer:** | well I mean, does it bother you, annoy you, I don't know, make you feel less content? |
| **Respondent:** | well I'm very much aware of slow Internet, but if it was an issue id just pay for a higher bandwidth |
| **Interviewer:** | ok. Would you ever be worried about your technical skill level in terms of troubleshooting a computer? |
| **Respondent:** | to a degree. Like some specialised software sometimes requires specialised technical support, so yes |
| **Interviewer:** | ok. Would you ever be concerned about computer viruses? |
| **Respondent:** | yes |
| **Interviewer:** | spam? |
| **Respondent:** | no |
| **Interviewer:** | any other concerns you have then that you can think of. |
| **Respondent:** | yeah maybe hacking and website security. I don't know a lot about that sort of stuff. And another thing, making your home computer child safe. Cos there is some crazy content stuff out there, and I don't like the idea of my kids finding it |
| **Interviewer:** | ok have you ever completed a CAPTCHA test? |
| **Respondent:** | no |

173

| | |
|---|---|
| **Interviewer:** | let me show you what a CAPTCHA test is... |
| **Respondent:** | oh yeah I have. I'm terrible at them. Frequently get them wrong |
| **Interviewer:** | ok and where are you seen them before. |
| **Respondent:** | I saw them when trying to get a new account. For email and maybe on Facebook. |
| **Interviewer:** | **H**ave you ever seen them on a blog? |
| **Respondent:** | oh yeah I have |
| **Interviewer:** | have you ever seen them when buying a ticket for an event online |
| **Respondent:** | yeah on Ticketmaster |
| **Interviewer:** | buying a ticket for a airline |
| **Respondent:** | yes. I mean I understand the concept of them. To stop bots getting a hold of too many tickets and stuff. I think I've seen it on Amazon too. |
| **Interviewer:** | so tell me more about your experience of using CAPTCHA. |
| **Respondent:** | I dislike it. I find it hard to read it, I get it wrong a lot, but I do understand the need for it. It will normally take me a couple of goes to get it right. I like the ones that use the two words... |
| **Interviewer:** | oh like reCAPTCHA? |
| **Respondent:** | Yeah, I find them a little easier to use. They help a bit |
| **Interviewer:** | so as you said CAPTCHA is used to show these websites that you are a human and not a robot. Another way of doing this would be to supply the website with a scan of our fingerprint, or face to allow the website to determine that we are human. But with this these websites would need to store our biometric information. So let's say both Google and the government implement a new feature whereby you can log into their online websites using your fingerprint and stuff. Would you be happy for Google to store a scan of your fingerprint? |
| **Respondent:** | No I wouldn't be happy. |
| **Interviewer:** | Even id this made your account more secure and less likely to be hacked |
| **Respondent:** | yeah, even if it meant that |

| | |
|---|---|
| **Interviewer:** | even if it meant you could log in quicker, as you wouldn't have to type in your username and password? |
| **Respondent:** | yeah, even then |
| **Interviewer:** | if it was mandatory.. |
| **Respondent:** | id leave. |
| **Interviewer:** | ok so what about the government. Would you give them your fingerprint information? |
| **Respondent:** | no. |
| **Interviewer:** | even though that by using this new feature you wouldn't have to use CAPTCHA on their website |
| **Respondent:** | I think I'd prefer to use CAPTCHA. I don't see a possible outcome of how the government could force me into it |
| **Interviewer:** | why would you not be comfortable with it? |
| **Respondent:** | because anything that's kept in a file format by someone can be hacked, and it's not that I think Google would misuse it, I just don't think they could keep it secure. Like if someone really wanted it they could get it. Government agencies especially. I mean you hear lads losing laptops that have private customer information on it. And I wouldn't be happy with anyone having that information. Cos someone could pretend to be me |
| **Interviewer:** | ok. Another way to identify yourself using voice recognition... |
| **Respondent:** | I wouldn't be happy with them having any information in a digital format that could uniquely identify me. |
| **Interviewer:** | ok, that answer will really speed up this interview. |
| **Respondent:** | that includes voice, that includes retina scan, that includes fingerprint. Any that is uniquely mine I want to keep it. |
| **Interviewer:** | what about handwriting? |
| **Respondent:** | well if you are going to place the same emphasis on handwriting, then yes I wouldn't like them to have it. Although like I have given the bank my signature to compare cheques, so what's the difference? |
| **Interviewer:** | yeah exactly |
| **Respondent:** | hmmm... i guess the physical world and the digital world are differnt. I guess I don't understand enough about the locks and |

175

safes that are involved. Physical lock I have more trust in than a firewall. Someone can break that firewall, but I don't think they'd break into the bank to get that information. So no I wouldn't trust them

**Interviewer:** have you ever signed your name electronically?

**Respondent:** yes, for DHL I think

**Interviewer:** and you were happy to do that?

**Respondent:** ermm... ha yes but now I'm wondering should I be or not. This is like everyone is out to get me. God. I suppose you give that information away all the time and don't even think about it. Especially with the cheque system, I mean your signature is key for that to work.

**Interviewer:** have you ever used a fingerprint scanner?

**Respondent:** no

**Interviewer:** have you ever been to the states

**Respondent:** yes

**Interviewer:** and you didn't have to give your fingerprint in immigration?

**Respondent:** no

**Interviewer:** not even ink?

**Respondent:** no, I don't think so. Maybe they did. I don't remember. But do they insist on it now?

**Interviewer:** yes

**Respondent:** well then I'd give it to them

**Interviewer:** so what makes that different then that giving it to log into a website?

**Respondent:** cos I can do without Gmail, but if I have to go to the states, then I have to go to the states. So it depends on leverage. My morals have leverage. And to be fair, when it gets to government rules I don't really have a choice.

**Interviewer:** but if you had a choice?

**Respondent:** erm... it's the storing I have a problem with. And the guys in the airport I suppose have to have it stored digitally if they comparing it against something.

| | |
|---|---|
| **Interviewer:** | well exactly, unless you are storing biometric information in order to compare it... |
| **Respondent:** | there's no point even having it |
| **Interviewer:** | exactly. |
| **Respondent:** | I don't like the information of it being stored, everything can be hacked. So id only be giving in that information if it was law. Otherwise id avoid it. |
| **Interviewer:** | ok I understand. You're not happy with it being electronically stored. That there are security risks with anything that is stored electronic. Potentially though, the government and site like Google are already storing a large about of data about you electronically already |
| **Respondent:** | yeah well. Yeah until such time, I'm flexible, that's my attitude now. If it's shown though that it can be secure I'd be happy to go along with it. |
| **Interviewer:** | do you use online banking? |
| **Respondent:** | yeah |
| **Interviewer:** | well it's would probably use similar secure that those online banking sites use |
| **Respondent:** | but that password isn't used on any other site. But if its biometrics and I used it for loads of websites, a person only has to get my fingerprint and suddenly they can get access to my bank details, my email, my Facebook, Amazon. I mean my whole online world would sudden open up to them. That's actually another difficulty I have with all this now that I think of it. I mean that would be very bad if that happened. Like they from knowing my biometrics that I use for Google, they could use the same to get into my bank.... and then with all my money... they could buy loads of ten penny bags. |
| **Interviewer:** | ha ha ok. So do you use Facebook? |
| **Respondent:** | yes |
| **Interviewer:** | do you have pictures of yourself |
| **Respondent:** | yes |
| **Interviewer:** | are you comfortable doing that? |

| | |
|---|---|
| **Respondent:** | I mean yeah. I don't like putting up pictures of my kids. But I don't mind putting pictures of myself up. |
| **Interviewer:** | so using face recognition would you be happy for the government to store that information? |
| **Respondent:** | well... no not to use of logging in. cos then someone just needs to hack into my Facebook, get a picture of me, and then use it to log into my bank account. |
| **Interviewer:** | so what if then you still had to log in using a username and password, but you just had to supply biometric information to show you were human. Would that change your option? |
| **Respondent:** | hmm... I mean I don't determine their policies. Would that change anything? Erm... id still be uncomfortable about it, ut maybe not totally against it. But I'd be worried that they would change their policies to use your fingerprint to log in, and I wouldn't be able to do anything about it. |
| **Interviewer:** | ok cool that makes sense. That's it anyway. Thanks |
| **Respondent:** | no problem |

**Female - 41**

| | |
|---|---|
| **Interviewer:** | so which of the following electronic devices do you own? A desktop computer |
| **Respondent:** | no |
| **Interviewer**: | a laptop |
| **Respondent**: | yea |
| **Interviewer**: | a tablet, like an iPad |
| **Respondent**: | no |
| **Interviewer**: | smart phone |
| **Respondent**: | yes |
| **Interviewer**: | music device |
| **Respondent**: | yes |
| **Interviewer**: | webcam |
| **Respondent**: | yes |
| **Interviewer**: | computer microphone |
| **Respondent**: | well that's built into the webcam is it not? So yeah |

| Interviewer: | how many hours a week do you spend using those electronic devices? |
|---|---|
| Respondent: | about 6 hours I think |
| Interviewer: | Which of the following activities have you performed on a computer? Email? |
| Respondent: | yes |
| Interviewer: | using word |
| Respondent: | yes |
| Interviewer: | writing a macro in excel |
| Respondent: | no |
| Interviewer: | writing a PowerPoint presentation |
| Respondent: | no |
| Interviewer: | playing compute games |
| Respondent: | no |
| Interviewer: | listening to or downloading music |
| Respondent: | yes |
| Interviewer: | online shopping |
| Respondent: | yes |
| Interviewer: | creating a website |
| Respondent: | well I have a blog. Does that count? I'd say yes |
| Interviewer: | ok. Developing computer software? |
| Respondent: | no |
| Interviewer: | in terms of computers and IT are you concerned about the age of any of your electronic devices |
| Respondent: | no |
| Interviewer: | do you get worried about slow internet access |
| Respondent: | no |
| Interviewer: | are you concerned about your computer technical skills |
| Respondent: | see would I worry about it? I don't think I would. But do I think I'd be able to do most things? I doubt it. |
| Interviewer: | ok that's fines. Are you concerned about viruses? |
| Respondent: | yes |
| Interviewer: | spam |
| Respondent: | not really no |

| Interviewer: | any other concerns that you can think about |
|---|---|
| Respondent: | I'm aware that sometimes when I'm searching for apples on the Internet, that maybe a week later it will start prompting me with adds about where I can find apples. And I just think that… there's a memory somewhere that's logging what I'm thinking. And I find that a little bit eerie sometimes. It's predicting my thoughts. It knows what I want to do before I do |
| Interviewer: | ok cool. Have you ever completed a CAPTCHA? |
| Respondent: | yes |
| Interviewer: | what were you doing when you came across it? |
| Respondent: | the last time I was trying to buy a ticket on ticket master |
| Interviewer: | ok how do you feel about CAPTCHA? |
| Respondent: | generally they're a pain. Because you can't read them. You could maybe do them 3 or 4 times before you get them correct. |
| Interviewer: | ok so CAPTCHA is used to show a computer that you are a human, and that you are not just some bot trying to spam the website. But there are other ways we could show the computer that we are humans. We could give the computer a scan of your face or fingerprint to prove you are human. This type of technology could then be used for, that instead of typing in your username and password or using a CAPCTHA you could scan in your fingerprint and get access to your, let's say, Gmail account or something. But with this, a company like Google would need to store your fingerprint information in their databases. Do you think that would be something that you would be comfortable with? |
| Respondent: | yes. |
| Interviewer: | Ok so let's say the government did the same thing. Maybe you could go online and log into your online tax account using your fingerprint information. Would you be happy with the government storing your fingerprint information? |
| Respondent: | oh well, sure if Google have it, you might as well give it to the Government |

| | |
|---|---|
| **Interviewer**: | ok. And if Google made it mandatory that to own a Gmail account you had to give in the same information |
| **Respondent**: | I don't know. Because, already people are talking about that you could do something stupid when you are 17, and you might want to forget about it and leave it behind when your older. I would be worried that it would be hard to do that if you had fingerprint. So I'd say no if it was mandatory. Like if I could opt in and opt out id be fine with it. But not if it was mandatory. |
| **Interviewer**: | and what if the Government made it mandatory. That to use this online service you had to give in your fingerprint information? |
| **Respondent**: | well I suppose it's the way forward. The Government? I'd be happier with them. I would think, or at least hope, that they would use the information wiser. |
| **Interviewer**: | ok so let's say Google made it mandatory but promised they weren't going to abuse the information, and that they'd use it correctly. Would you be happy then? |
| **Respondent**: | I don't know. This is a real quandary. I just don't know. It's very personal. It's like creating a DNA database. So, no. |
| **Interviewer**: | but you'd be happy to give it to the Government? |
| **Respondent**: | hmm... no actually, I don't think I would. |
| **Interviewer**: | even if they promised |
| **Respondent**: | I'd give it to Enda. Ha. Ok yeah maybe the government, but not Google |
| **Interviewer**: | have you ever had to give your fingerprint to someone before |
| **Respondent**: | once |
| **Interviewer**: | what were you doing that for? |
| **Respondent**: | going through passport control through Shannon. Getting into the States. They make you give it in there |
| **Interviewer**: | and you were happy with that |
| **Respondent**: | eh… yeah, but I had no choice. I don't intend to break the law so I should be ok with them having that information |
| **Interviewer**: | desperate times…. |
| **Respondent**: | yeah well, but I have actually thought that there is a use to DNA stuff. Like it serves a purpose. So I really shouldn't be against it. |

| | |
|---|---|
| **Interviewer**: | that's true. Ok so another way to identify you is to use voice recognition. Would you be happy to give that information to Google? |
| **Respondent**: | yes |
| **Interviewer**: | and why do you feel differently with the voice and the fingerprint |
| **Respondent**: | erm… I think it's just not as personal. Fingerprint is so so unique; you're giving away a piece of yourself. But the voice is less unique. |
| **Interviewer**: | yeah makes sense. And for the Government to store the same information? |
| **Respondent**: | yes I'd be happy with that |
| **Interviewer**: | ok. Have you used voice recognition before? Like on your phone or anything? |
| **Respondent**: | oh yeah yeah I have |
| **Interviewer**: | and how do you find it |
| **Respondent**: | eh… it's ok. It's not the smartest. You have to talk slow with an American accent. So it's not great |
| **Interviewer**: | ok. So another way identify someone is using face recognition. And for this to work Google or the government would have to store a picture of your face. Would you be happy for Google to have that information? |
| **Respondent**: | no |
| **Interviewer**: | why? |
| **Respondent**: | because I'm a girl and I might not have my hair done that day. The shadows might be showing… vanity really |
| **Interviewer**: | ok, and would you be happy for the government to have that information? |
| **Respondent**: | no |
| **Interviewer**: | do you own a Facebook page? |
| **Respondent**: | yes |
| **Interviewer**: | and do you put pictures of yourself up on that? |
| **Respondent**: | ah you caught me out there. |

| | |
|---|---|
| **Interviewer**: | ha ha well no I mean you might feel that they're different. And I'd like to know what the difference is for you |
| **Respondent**: | I have a distant view picture. I have no close up pictures. I get to choose those pictures. And I don't let people tag me. I mean I've seen those people who put up millions of photos and they're so random. And they look horrible in them. I don't want pictures up like that with me in them |
| **Interviewer**: | ok and do you have a passport |
| **Respondent**: | yes |
| **Interviewer**: | and you have a picture on those |
| **Respondent**: | yes |
| **Interviewer**: | and you were happy to give it to the Government |
| **Respondent**: | well yeah. I mean I had to. And they're not going on the Internet to be spread all over the place. So it's staying in one office for one use only. Internet pictures are different though |
| **Interviewer**: | another way to identify yourself is through an iris scan. Would you be happy for Google to have that information? |
| **Respondent**: | no |
| **Interviewer**: | and the government |
| **Respondent**: | no |
| **Interviewer**: | why not for both |
| **Respondent**: | I think it's just privacy. It's taking it too far |
| **Interviewer**: | ok last one. Handwriting, you can use that to identify yourself. Would you be happy for Google to have that information? |
| **Respondent**: | yes I think so |
| **Interviewer**: | and the government? |
| **Respondent**: | yes |
| **Interviewer**: | have you ever had to sign your name electronically? Maybe for the post or something? |
| **Respondent**: | no, I don't think so |
| **Interviewer**: | ok that's perfect, that's all I need to know. Thanks |
| **Respondent**: | great |

**Male - 32**

| | |
|---|---|
| **Interviewer**: | ok so are you familiar with CAPTCHA and what it is used for? |
| **Respondent**: | yeah, sure it's used to tell if you are a human or not |
| **Interviewer**: | yes exactly. |
| **Respondent**: | like they sure a good purpose in stopping spam and all, right? |
| **Interviewer**: | yeah definitely, but potentially there are other ways you could show you are a human to a computer. By using biometric information. So let's say you could sign into your Gmail account using your fingerprint scan and get access that way. Or even if you were checking your PAYE account online you could do the same. But this means that either Google or the government would need to store this biometric information on their databases. |
| **Respondent**: | ok |
| **Interviewer**: | so would you be happy for Google to store your fingerprint information? |
| **Respondent**: | yeah I would |
| **Interviewer**: | and the government? |
| **Respondent**: | eh yes. I would be happy for them to have the information as well. Primarily because the government, well the information would have to be used properly, and it is going to be used properly by the government anyway so, they have all your details anyway. You trust them with your passport and your driver's license so all that kind of stuff. So I don't have a problem with them having my biometrics |
| **Interviewer**: | would you trust Google and the government on the same level? |
| **Respondent**: | eh… I probably would yeah. I mean it's very small section of information, and the ability to abuse that information, has to be marginal |
| **Interviewer**: | have you ever used a fingerprint scanner? |
| **Respondent**: | yeah in the airport, and security checks in the UK. I think the thing is that with any entitlement you have to give something. And if you don't want to give them that information that's fine, it just means you're not entitled to the entitlement. |

| | |
|---|---|
| **Interviewer**: | sure ok. So if it the fact that it is an option for you that you are happy to give it in? If it was mandatory. |
| **Respondent**: | I'd have no reservation anyway. But Google and government, in fact any service providers are perfectly in their rights to impose any provisions they like on you. I really don't see it as a problem |
| **Interviewer**: | what about face recognition. Are you happy to give a picture of you face to Google? To the Government? |
| **Respondent**: | yes, and strangely enough id feel more comfortable giving a picture to Google as opposed to Facebook. |
| **Interviewer**: | and why is that? |
| **Respondent**: | I don't know. I have no idea. I think Google have always been very open about their security policies. I'm not sure the same can be said for Facebook. |
| **Interviewer**: | ok. That's fair enough. Ok so you seem to be very open with all of these things. Would you be happy on the same level with retina scanning, iris scanning, voice, handwriting? |
| **Respondent**: | yes absolutely. That information is out there anyway. I mean for both the passport and drivers license you provide a sample of your signature. I think the state should reserve the right to get any information that they want, and as for Google it's a service. So if you don't want to comply with their rules, then get your email from elsewhere. |
| **Interviewer**: | have you ever given in your signature |
| **Respondent**: | yes. To An Post. |
| **Interviewer**: | and from a usability point of view you were happy to use it. |
| **Respondent**: | yeah. I'm not sure if the electronic sample I provided though would actually be the same as my written one. I find it different to use |
| **Interviewer**: | absolutely. So cool that's all I needed to know. Thanks |

**Female – 34**

| | |
|---|---|
| **Interviewer**: | have you ever used CAPTCHA before? |
| **Respondent**: | Yes I have and I hate them so much. |

| | |
|---|---|
| **Interviewer**: | Why is that? |
| **Respondent**: | Because I can't read them at all. I always get my fiancée to do them for me when I'm like buying a plane ticket or on… where else has them… like Ticketmaster and stuff. I just can't make them out. Like I'll try some of them if I feel they're easy, but most of the time I fail at them, and get however is sitting near me to do them. |
| **Interviewer**: | so there's a possibility out there, that instead of using CAPTCHA, a person could bypass that mechanism and sign into maybe a Gmail account, or a PAYE account using biometric data that they supplied using the appropriate scanner. So like you fingerprint could be used, your voice and so on. But with this, this biometric data would have to be stored on either, in this case, Google's database or the government's database. Would you be comfortable with Google storing your fingerprint information so that you could use it to sign into you Gmail account? |
| **Respondent**: | yeah |
| **Interviewer**: | and the government? |
| **Respondent**: | yes |
| **Interviewer**: | what if Google turned around and said that you had to supply this information, otherwise you wouldn't be allowed to have a Gmail account? Would that change your mind? |
| **Respondent**: | it depends on the terms and conditions if I'd use it. I might weight up the alternative services as well, and then decide. |
| **Interviewer**: | so if they promised in their terms and conditions that they wouldn't spread this information around or use it incorrectly? |
| **Respondent**: | I'd still have a look around to see if there were other similar services that didn't need your fingerprint information. Like if there was no viable alternative, I'd consider it, but I'd be worried about the reason why they wanted to make it mandatory. That would sound a little dodge to me. And what they promise now might not be what they promise in a few years down the line. |

| **Interviewer**: | So you would or wouldn't be happy with them having this information if it was mandatory? |
|---|---|
| **Respondent**: | I wouldn't I suppose. I definitely look for an alternative. |
| **Interviewer**: | have you used a fingerprint scanner? |
| **Respondent**: | in airports and stuff |
| **Interviewer**: | and you were happy to use them? |
| **Respondent**: | well not really, but I don't have a choice. I mean I want to go to the states and see my family, so I have to give them my fingerprint. But I don't have to use Gmail. I could just use hotmail or something. |
| **Interviewer**: | would you be happy giving Google a picture of your face so you could bypass CAPTCHA? |
| **Respondent**: | same answer as before. Like I'd rather not, but I don't care enough to say no. I'd be less concerned about that one I think? |
| **Interviewer**: | why is that? |
| **Respondent**: | because, just initial reaction. I haven't really thought it through. |
| **Interviewer**: | well that's great. Do you want me to let you think about it and come back to that question? |
| **Respondent**: | no I mean initial reaction I wouldn't be as concerned because I don't think that your face is as unique. Like the fingerprint it very unique. If you are out in public your photo can be taken by anybody and with all the CCTV cameras out there already scanning your face so. I kind of think that's already happening. Again, I'm not as bothered about it, but if there was another email service out there that didn't need this information I would move to using that instead |
| **Interviewer**: | ok but let's say it wasn't mandatory and giving this information meant that you could get around using CAPTCHA. Would you be more open to it then? |
| **Respondent**: | well I don't know. Like CAPTCHA is a pain, but I'd love if there was another way to get around it without having to give my biometric information |
| **Interviewer**: | do you have a Facebook account? |
| **Respondent**: | yes |

| Interviewer: | and you're happy to put pictures up of yourself? |
|---|---|
| Respondent: | no I don't, but other people do and tag me |
| Interviewer: | and you're ok with that? |
| Respondent: | I'm mean as happy as you can be I suppose |
| Interviewer: | so what's the difference then in Facebook having your picture from Google? |
| Respondent: | well there is no difference is there? It's just another corporation really. I'd rather them not have that information, but I've given it to Facebook for social reasons, cos I wanted to share those photos with people. Whereas Google would want it to use for authentication. So I feel that's different. One is for social reasons and the other is for security reasons. |
| Interviewer: | and if Facebook wanted to use those photos that you have already uploaded for security reasons, would you be happy with that? |
| Respondent: | I'd be concerned then. Cos with just looking at the photos, the worst that could happen is I could be doing something stupid, but with security, the worst that could happen is someone could access all my accounts by faking my biometric information. That's a lot more worrying |
| Interviewer: | what about the government storing a picture of your face? |
| Respondent: | well I think they already do. I wouldn't happy for them to share it. But I wouldn't be comfortable with the government having online databases with this information on it. So I'd say no. |
| Interviewer: | yeah absolutely. So voice recognition, would you be happy for Google to store a sample of your voice? |
| Respondent: | I'd be more comfortable with the username and password that we use today than with using voice. I wouldn't have any desires to switch to voice. Again it would be a reason for me to move away from Google |
| Interviewer: | if the government wanted it? |
| Respondent: | well I think the same security issues exist. The Government can't guarantee the security of your information anymore than Google can. So I'd rather not. |

| | |
|---|---|
| **Interviewer**: | what about storing your handwriting to identify yourself. Would you be happy to give that information to Google? |
| **Respondent**: | signature is used for a lot of things. Like credit cards. So I'd be concerned with sharing out that information. Like if someone got hold of that information, they could potentially take out my money and use my cheques. So I wouldn't be happy with that. Whereas if someone got my Google password, I think the person would be limited to the damage they could do. So I'd rather stick with a password. |
| **Interviewer**: | and the government? |
| **Respondent**: | I think they already have it. But the same concerns apply. It's just not secure. |
| **Interviewer**: | ok so I presuming then that you'd feel the same for iris scanning? |
| **Respondent**: | yeah, exact same. |
| **Interviewer**: | Regarding the signature, have you ever had to sign for something electronically? |
| **Respondent**: | yes |
| **Interviewer**: | and you found it ok? |
| **Respondent**: | oh well I find it very poor. The way I sign in real life is very different than how I sign on those things. Like it feels a little different than writing with a pen. I don't think I really sign the same using a stylus and stuff. |
| **Interviewer**: | why is that? |
| **Respondent**: | don't know just different weight and texture. Even there's a different resistance, but in saying that I don't do it often enough. If I did it more I'm sure I'd get better at it. |
| **Interviewer**: | and you were happy to give them your signature in digital form? |
| **Respondent**: | well I was at the time. But now I'm thinking I should have been more negative about it. But these things have a way of creeping up on you. You give out the information without even thinking about it. |
| **Interviewer**: | yeah absolutely. Well that's all I needed. Thanks |
| **Respondent**: | no problem. Best answers ever. |

**Male - 26**

| | |
|---|---|
| **Interviewer**: | which of the following electronic devices do you own? A desktop computer? |
| **Respondent**: | no |
| **Interviewer**: | laptop? |
| **Respondent**: | yes |
| **Interviewer**: | tablet? |
| **Respondent**: | yes |
| **Interviewer**: | smart phone? |
| **Respondent**: | yes |
| **Interviewer**: | webcam? |
| **Respondent**: | yes |
| **Interviewer**: | microphone? |
| **Respondent**: | yes |
| **Interviewer**: | music device? |
| **Respondent**: | no |
| **Interviewer**: | how many hours a week do you spend using those devices. |
| **Respondent**: | 60 plus id say |
| **Interviewer**: | which of the following activities have you performed on a computer… email? |
| **Respondent**: | yes |
| **Interviewer**: | word? |
| **Respondent**: | yes |
| **Interviewer**: | PowerPoint? |
| **Respondent**: | yes |
| **Interviewer**: | macro in excel? |
| **Respondent**: | Marco in excel? No |
| **Interviewer**: | surfing the Internet? |
| **Respondent**: | yes |
| **Interviewer**: | shopping online |
| **Respondent**: | yes |
| **Interviewer**: | computer games |
| **Respondent**: | yes |

| | |
|---|---|
| **Interviewer**: | downloading or listening to music? |
| **Respondent**: | yes |
| **Interviewer**: | developing a website |
| **Respondent**: | yes |
| **Interviewer**: | developing computer software? |
| **Respondent**: | yes |
| **Interviewer**: | any in particular that concerns you with computers, technology, IT? |
| **Respondent**: | recording of my personal data. |
| **Interviewer**: | that bothers you? |
| **Respondent**: | yeah definitely. I think about that a lot |
| **Interviewer**: | would you get concerned about slow Internet? |
| **Respondent**: | yes |
| **Interviewer**: | virus or spam? |
| **Respondent**: | No |
| **Interviewer**: | why not? |
| **Respondent**: | I don't use an operating system that is susceptible to computer viruses |
| **Interviewer**: | have you ever used CAPCTHA before |
| **Respondent**: | yes |
| **Interviewer**: | where? |
| **Respondent**: | when logging into websites |
| **Interviewer**: | which websites |
| **Respondent**: | well mostly when I put the password in wrong |
| **Interviewer**: | can you think of a website where that has happened to you? |
| **Respondent**: | Gmail. Facebook. Actually Facebook have funny ones, like identify these friends and stuff. And wordpress comments |
| **Interviewer**: | ever buy a ticket on Ticketmaster? |
| **Respondent**: | don't think so |
| **Interviewer**: | ever see it on an airline website? |
| **Respondent**: | yes |
| **Interviewer**: | and how do you feel about them? |
| **Respondent**: | sometimes tricky. Sometimes frustrating |
| **Interviewer**: | in what way? |

| | |
|---|---|
| **Respondent**: | multiple failures. |
| **Interviewer**: | ok. You know you can talk freely here. You don't have to give me bullet points. I don't mind having to type it up after. You're bullet pointing me |
| **Respondent**: | ok |
| **Interviewer**: | So who do you feel about CAPTCHA |
| **Respondent**: | I feel ok about them. Like I don't mind using them. Really |
| **Interviewer**: | ok. So some people do have problem with CAPCTHA, so a way for them to get around CAPCTHA but still prove they are human would be to supply a website with their biometric information. Like so maybe to log into your Gmail account you could give in your fingerprint, or to pay for bin tags online, you could log into a government run site with your fingerprint. Obviously this means though that a company like Google, or the government would have to store that information. Do you think you would be happy for Google to store your fingerprint information in their database? |
| **Respondent**: | eh I'd be a bit concerned about that. |
| **Interviewer**: | why? |
| **Respondent**: | because I don't feel that information should be given to a private organization? |
| **Interviewer**: | why not? |
| **Respondent**: | cause it could get hacked. Or copied and then your passport could be forged. |
| **Interviewer**: | but even if it meant that your Gmail account would be less likely to be hacked, because you were using fingerprint recognition? |
| **Respondent**: | I still wouldn't be happy. I don't think the pros out weight the cons. |
| **Interviewer**: | what if Gmail turned to your tomorrow and said you can't have a Gmail account unless you give us this information? |
| **Respondent**: | I'd only be happy if it was the norm for everyone else. Like if Google were going out on their own but other places like yahoo |

|  |  |
|---|---|
| | weren't, then I'd go to yahoo. But if everyone was doing, I'd give Google the information |
| **Interviewer**: | ok what about giving this information to the Government? |
| **Respondent**: | well they already have this information. So yes I'd be happy with it. |
| **Interviewer**: | have you ever used a fingerprint scanner before? |
| **Respondent**: | yes in American immigration. |
| **Interviewer**: | and you were comfortable with that |
| **Respondent**: | yes |
| **Interviewer**: | ok so another way to identify yourself is using voice recognition. Would you be happy for Google to have that information? |
| **Respondent**: | yes. They probably have it already |
| **Interviewer**: | why do you think that? |
| **Respondent**: | because I use Google voice from time to time |
| **Interviewer**: | so why are you happy to give out that information and not your fingerprint? |
| **Respondent**: | cos your voice isn't necessarily unique. Well I don't know the ins and outs, but fingerprint is very personal, but voice not so much |
| **Interviewer**: | what about the government having that information? |
| **Respondent**: | yes. I'd be happy with that |
| **Interviewer**: | ok another way is iris scanning. Would you be happy with Google having that information? |
| **Respondent**: | well no. I think the same rules apply with the fingerprint |
| **Interviewer**: | and why is that? |
| **Respondent**: | it's just in the same category in my head |
| **Interviewer**: | and the government? |
| **Respondent**: | yes |
| **Interviewer**: | is there anything Google could do to change your mind? |
| **Respondent**: | I can't think of anything off hand. |
| **Interviewer**: | ok. |

| | |
|---|---|
| **Respondent**: | maybe if there was some way that Google didn't have the information. Like they could just proxy the information through the government or something. |
| **Interviewer**: | ok so you'd be happy for Google to use the information but just not to store it? |
| **Respondent**: | yes as long as Google agreed not to store any of the data I'd be happy with that |
| **Interviewer**: | ok. So face recognition is another one. Would you like Google to store a picture of your face? |
| **Respondent**: | yeah I think so |
| **Interviewer**: | so why are you comfortable with that? |
| **Respondent**: | cos my face is everywhere. There's nothing private about my face |
| **Interviewer**: | what is your face on? |
| **Respondent**: | Gtalk, msn, Google+, Facebook |
| **Interviewer**: | and why are you comfortable putting that information out there like that? |
| **Respondent**: | cos I think it's like… my fingerprint and my signature are very unique. My face isn't. Like I wouldn't want my signature to be out on the internet? |
| **Interviewer**: | why? |
| **Respondent**: | because then people could be forging documents. |
| **Interviewer**: | so but back to the face, you'd be happy for Google and the government to have that information? |
| **Respondent**: | yeah |
| **Interviewer**: | ok so then with your handwriting, you wouldn't be happy with Google having that information |
| **Respondent**: | no. not with identity theft |
| **Interviewer**: | and the government? |
| **Respondent**: | I think they already have it |
| **Interviewer**: | and are you happy with that |
| **Respondent**: | yes |
| **Interviewer**: | so why are you more comfortable with the government having it and not Google? |

| | |
|---|---|
| **Respondent**: | cos it's not a private organization that could misuse the data |
| **Interviewer**: | so you trust the government? |
| **Respondent**: | well, not… from a IT stand point not as much as Google, but from a moral standpoint probably more |
| **Interviewer**: | ok makes sense. Have you used an electronic signing devices? |
| **Respondent**: | yes |
| **Interviewer**: | what were you doing? |
| **Respondent**: | signing for my credit card in some shop |
| **Interviewer**: | and you were happy with that |
| **Respondent**: | well I'm not sure what value it gives. Like it wasn't a legible signature. |
| **Interviewer**: | if your signature normal legible? |
| **Respondent**: | ha no, not really |
| **Interviewer**: | but you were comfortable giving it |
| **Respondent**: | yes |
| **Interviewer**: | so why is that? |
| **Respondent**: | not sure. Maybe at the time I didn't really think about it. If I could switch to using chip and pin I probably would have. But I couldn't. |
| **Interviewer**: | ok that's perfect, thanks |
| **Respondent**: | that's it? Ok cool. |