Online Privacy and People's Awareness: A Study of Irish Students

Elaine Colfer B.Sc. (Hons)

A Thesis Submitted for the Masters in
Computing in Information Systems Processes

School of Science
Department of Computing, Maths and Physics
Waterford Institute of Technology

Head of Department:	Dr. Mícheál ÓhÉigeartaigh
Research Supervisor:	Ruth Barry
	Liam Doyle

Submitted to Waterford Institute of Technology

October 2007

Acknowledgements

I would like to thank my parents, Helen and Brendan. They are responsible for me getting this far in my education and in life. With thanks for being my personal bank.

My siblings Sarah and Mark, with special thanks to Sarah for all the help and Mark for not listening.

I would like to thank the rest of my family and friends especially Caroline, Róisin and Christine. Also Benny thanks for bullying me into doing the masters.

Finally thanks to my supervisor Ruth Barry and my course leader Liam Doyle.

Declaration

I hereby certify that this material which I now submit for assessment on the programme of study leading to the award of M.Sc. in Computing in Information Systems Processes is entirely my own work and has not been submitted in whole or in part for assessment for any academic purpose than in fulfilment for that stated above.

Signed …….. ..……..…… Date ……..

Table of Contents

Chapter Three Research Methodology

Chapter Four Findings

Chapter Five Conclusion

References

Abstract

This study investigates the awareness levels of college student's views on possible software tools that can gather their personal information online. A review of the current literature demonstrates three possible tools that can gather people's personal information online. Following this, possible methods of protection available to Internet users are identified.

This study employs quantitative research using questionnaires to examine Internet privacy awareness levels among 70 college students. Analyses of the results of questionnaires administered to college students, suggests that there is a relatively high level of knowledge of possible software tools that can invade their privacy online. The results indicate major differences in the views of male and female participants in relation to privacy online with 73.5 per cent of male rating convenience over privacy. Also highlighted in the study is the varying awareness levels between students of different areas, students from the business school have a greater knowledge of possible software tools that can invade their privacy in comparison to humanities students.

List of Tables

List of Appendices

Chapter One:

Introduction

1.1 Introduction

Privacy has always been a conversational topic long before the advent of technology but with the development of computers and the Internet it has been pushed more into the limelight and has become a heated topic for debate. Since computer technology became widely used in the 1960's, people have been discussing ways in which personal information is stored, collected, processed and used by both governments and large organisations. The capture of this data led articles to be written about the surveillance state that was developing (Cavoukian & Tapscott; 1995; Stone & Warner; 1970)

In the 1970's, the consensus appeared to be that there was potential for the surveillance to lead to a "Big Brother" (Orwell, 1984). Many books were written during this decade portraying the dangers of the concept of "databanks" that were being developed by government projects (Stone & Warner; 1970)

Privacy concerns have altered since this time and the 1990's saw possible surveillance coming from both the private and public sector. The concept of "Big Brother" was generally replaced by a "data trail" that individuals leave behind them innocently and unknowingly while using the Internet to carry out every day innocent tasks (Cavoukian & Tapscott; 1995)

When considering privacy online it must be noted that the levels of advancement in technology in the previous fifteen years have lead to this problem. The very technologies that are allowing people to carry out transactions over the Internet also cause the main source of privacy violations. The increased usage and availability of broadband for Internet access to carry out daily responsibilities from chatting to an old friend to paying a bill has meant that more and more of people's lives are being conducted online. This leads us to presume that people are becoming more

dependent on technology and whether are they aware of potential threat to their privacy online.

1.2 Need for study

In recent times as more and more people use the Internet to carry out everyday activities the problem of identity theft has become a cause for concern as personal information is stored on different websites (Dasgupta & Turner, 2003; Nissenbaum, 1998). This again assumes that people are not fully aware of how their privacy can be invaded while they are online.

The ways in which people's privacy may be invaded can vary from a company having a security breach to the use of software these companies implement like "cookies", "spyware" and "web bugs" to find this information (Bennett, 2001; Chung & Paynter, 2002; Fonseca, 2005; Kucera et al, 2005).

This study will investigate a generation where using the Internet to carry out their every day lives is the norm. Even though the majority of the population in this study are very comfortable with using the Internet, awareness will be investigated to find out their knowledge of how their personal information is assembled, analysed and stored by third parties online. The software used to invade privacy and tools used in gathering people's personal information will also be explored.

1.3 Research objectives

Based on the knowledge of previous studies and the growing usage of the Internet for everyday duties (Graeff & Harmon, 2002; Nissenbaum, 1998) the literature shows a need to investigate people's perception on Internet privacy, their awareness of what technological tools could invade their privacy online and how these tools collect and store their information (Bennett, 2001; Dasgupta & Turner, 2003; Graeff & Harmon, 2002; Kucera et al, 2005). The target population is college students in this study. College students are chosen for many reasons including easy access and their assumed proficient use of the Internet. The research objective for this study is set out below:

Research Objective:

> To measure the target population awareness levels of Internet privacy and possible software and tools used by companies to gather their personal information online.

Following on from the research objective two sub objectives were developed, which were as follows,

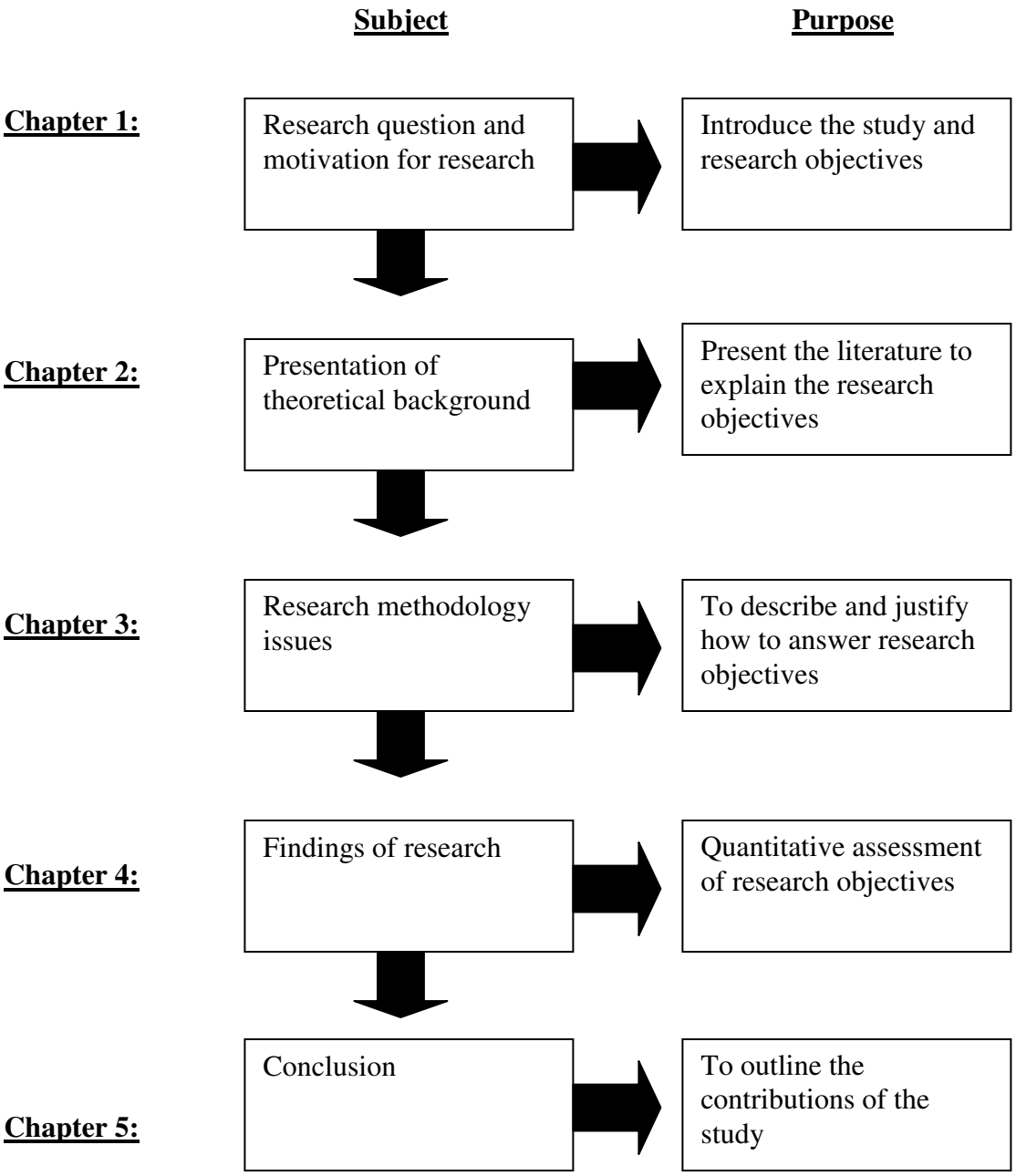
- Which is more important convenience or privacy in term of male and female users?

- Are there different levels of awareness of possible threats to online privacy dependent on the student's area of study?

1.4 Thesis Structure

In this section a brief outline of the remaining chapters will be given. Chapter two will contain the literature review which explores the ways in which privacy is invaded in an online environment. The different methods for the invasion of privacy are investigated along with the potential ways that companies may use the information gathered. The chapter concludes with an examination of potential ways in which people's personal information can be protected online. The third chapter discusses the research methods for the investigations carried out in this study. In chapter four an analysis of the research carried out is presented. In the fifth chapter conclusions are drawn out and possible future directions for research are proposed.

1.4.1 Overview of this Thesis



1.5 Conclusion

Within this chapter the issue of Internet privacy was introduced. The need for this study is justified with the main reasoning being the increased usage of the Internet to carry out daily tasks and the awareness levels of people about how their personal information can be invaded (Dasgupta & Turner, 2003; Graeff & Harmon, 2002; Nissenbaum, 1998). Also, included in this chapter is the research objective. The chapter ends with an outline of the following chapters in this thesis.

Chapter Two:

Literature Review

2.1 Introduction

Privacy has been an issue for many people for a long time but with the development and increased usage of the Internet it has become a bone of contention for many more people. According to Scott McNealy[1] (1999) "You already have zero privacy. Get over it" (Baig et al, 1999). It is assumed by Scott McNealy (1999) that we have no privacy and need to get used to this fact. If this is the case how can people be protected. This chapter will provide an overview for some of the privacy issues that Internet users face everyday and ways to overcome them. The first section begins with a brief look at the history of the Internet. Followed by how a person's personal information is gathered and an example of one company's dealings with people's personal information. An overview of protection methods available is then provided.

2.2 A brief history of the Internet

The Internet is a cause for concern regarding online privacy, therefore it appears to be relevant to give a brief overview of the Internet, how it began and how it developed over the decades (Caudill & Murphy 2000).

The first signs of the Internet appeared in 1969, when the Pentagon's Defense Advanced Research Projects Agency (DARPA) considered a way to develop a reliable communications network with multiple-backups to survive a nuclear war. At the time this seemed way beyond the capabilities of the current network technology that was in place. The Internet began with four nodes each with equal authority to send, receive and originate messages, with the first machine installed in

[1] Scott McNealy was the CEO of Sun Microsystems Inc. at the time of his comment.

UCLA in 1969. The four machines transferred data on dedicated high speed transmission lines (Sterling, 2005).

Right through the 1970's the network grew, assisted by the spread of the personal computer. The decentralised structure made expansion achievable with greater ease as it could accommodate many varying kinds of machines. It could be said that in 1984 one of the first steps in developing the Internet as we know it, occurred when the Pentagon gave up their control over it. In May 1994, the National Science Foundation (NSF) announced plans to hand over the Internet to the private sector, this hand over did not occur until April, 1995. The major steps above paved the way so that the Internet could become what we know it as today (Sterling, 1995; Mujtaba, 2003).

Internet usage has grown so rapidly for many reasons. First the 1990's saw significant price decreases in the equipment required to gain access to the Internet. One of the most obvious reasons for the popularity and growth of the Internet is the freedom it offers people. People can communicate with almost anyone they wish or explore and seek information about almost anything imaginable to mankind. The price of Internet access is also falling in most developed countries while the availability of the Internet is starting to grow in developing countries. The growth of the Internet is highlighted in appendix one taken from the Internet World Stats information Website. The percentage of Internet users will only grow as other countries in the world start to develop more. In an Irish context, the level of Internet usage growth, as a percentage of population has more than doubled since 2000 (See appendix two). There is nobody to protect the information on the Internet or protect those who use it. This leads to major problems in the regulation and supervision of the Internet (Mujtaba, 2003). There have been attempts within individual countries to try regulating the Internet but as it is a global phenomenon this has proved futile.

The usage of the Internet to carry out daily tasks like grocery shopping and banking has made protecting people's privacy online more challenging (Nissenbuam, 1998;

Milne & Rohm, 2000; Broom et al, 2002; Dasgupta & Turner 2003; Broadhurst, 2006). As people continue to increase their usage of the Internet for every day items, individuals will and are becoming more concerned with how to protect their privacy online. People's perception of how safe they are online will continue to develop along with a tendency to wonder what's in place to protect them (Dasgupta & Turner, 2003).

Almost all computer based activities have jargon attached and the Internet is no different. Therefore, the most prolific of these will be explained below. These focus on the terminology surrounding websites. Websites are accessed by using a web browser that is used to display and locate websites. Websites are found on the Internet by using a uniform resource locator (URL). A URL is the way to specify the location of anything on the Internet and acts like a global address. Websites are developed using the hyper text mark-up language (HTML), an authoring language used to create websites. HTML is normally inserted into text files. HTML is made up of tags, which highlight the features within HTML. A homepage can refer to either the first page on a website or what website opens when a user clicks on their browser to access the Internet (Downing et al, 2000; Webopedia.com).

The Internet is accessed through an Internet Service Provider (ISP) company; these are companies that charge a fee for access to the Internet. The Internet communicates using a protocol called the transmission control protocol/ Internet protocol (TCP/IP). TCP/IP is used to connect hosts on the Internet. Hosts are when two computers are connected via modems and the computer that holds the information is called the host. The Internet also has a separate protocol for the transfer of files called the file transfer protocol (FTP). FTP is a standard way to transfer files between computers on the Internet over TCP/IP networks (Downing et al, 2000; Webopedia.com).

2.3 How personal information is gathered?

When you turn on your television and watch your favourite program no one is looking over your shoulder taking notes on what you do. When you go for a stroll around the shops no one is following you to take notes on which shops you enter and which you walk away from. When you log on to the Internet it should not be any different – but it is. Websites with the aid of software are looking at your every move while you are online. A Harris interactive survey in (2000) as cited by Bennett (2001), found that 56 per cent of adults who responded were very concerned about a loss of personal privacy. The loss of personal privacy was rated above topics such as crime. Below is a brief look at some of the methods that are in use.

2.3.1 Cookies

A cookie in computing terms was originally designed and developed to overcome the stateless nature of the HTTP protocol. A cookie is a piece of information passed between an Internet server and a user's web browser. A cookie is normally a text file. The text file is sent from a web server to a browser to enable the server to identify the web user at the current time. The web server has the ability to identify a web user through a unique identifier. A unique identifier is a number given to the web user that is only relevant to that web user that can be used to identify them online at any time (Beise et al, 2001; Cunningham, 2002; Kierkegaard, 2005).

There are two main types of cookies; these are persistent cookies and session cookies. Session cookies only remain active until a user exits a website window. These cookies do not cause much concern for many. The concerns with cookies come from persistent cookies. Persistent cookies have an expiry date and time and remain active on a user's hard drive until they expire or until the user deletes the files (Beise et al, 2001; Kierkegaard, 2005). It has been found that some Internet users are unaware of the automatic collection of personal information via persistent

cookies (Beise et al, 2001). The study also shows that those who are aware of persistent cookies consider them a threat to privacy.

2.3.1.1 What cookies do?

Cookies have many functions and can do many things online, both good and bad. According to Cunningham, 2002; Geer et al, 1997; Goldsborough, 2005, the three most common functions of cookies tend to be:

- help identify the habits of a user
- track the login status of users
- track website's and pages visited on a specific website's

A cookie can track the habits of a particular browser at a given IP address. The cookie can only fully identify the user if and when the user logs into the website. Once the user is identified it is possible to find out what website pages the user visits to build up a picture of what a particular user is doing online (Cunningham, 2002; Geer et al, 1997; Goldsborough, 2005).

Website developers use cookies to examine what pages a user clicks through on a website and how they use it. Once this information gathered by the cookie has been examined in detail by the website's developers, it can be used to develop more functional and easier ways to navigate their websites. Many would believe that this is a legitimate use for cookies as it does not adversely affect the user of a website, in fact it may aid them in the future (Cunningham, 2002; Geer et al, 1997; Goldsborough, 2005).

Perhaps one of the most helpful usages of cookies can also be one of the most dangerous. This is a cookie that tracks the login status of a user on a particular website. It is useful in an obvious way as the user does not have to login into the website every time they wish to use it. It can also be very dangerous as the

information is stored in a cookie file meaning it can be accessed by an unauthorised third party. If an individuals username or password is accessed by a person who could abuse it, serious outcomes could occur. This is becoming a major problem with the usage of Internet banking (Cunningham, 2002; Geer et al, 1997; Goldsborough, 2005).

2.3.2 Web bugs

Web bugs are a newer form of tracking devices used on websites. Web bugs have started to become a more device for of tracking individuals online as people have become more aware of how to protect themselves from cookies. Web bugs are hidden within websites and can only be found if the HTML is examined. Within the HTML code, the web bugs is shown in the "img" HTML tag. Web bugs can also be hidden in Microsoft Word documents, e-mail messages and many other HTML documents. A web bug is normally one by one pixel in size and has no colour. A web bug works when a user visits a website or activates a web bug in some way. The user's web browser automatically requests them, therefore the user's IP address is sent to the host. Several other pieces of information are also sent with the IP address. In addition the URL is sent, known as a web address of the web bug image, along with the time the web bug was viewed and the specific browser type. While carrying out a review of the literature in this area, it became apparent that there are no reliable studies into the Internet user's views on privacy (Bennett, 2001; Chung & Paynter, 2002; Fonseca et al, 2005; Smith, 1999).

2.3.2.1 What web bugs do?

Web bugs as with cookies were originally developed to aid the Internet user. An original use of web bugs was that it made it possible to track where documents go when it leaves the author's hand. This could aid a copyright holder track where the

document has gone and stop any copyright infringement. As copyright infringements are illegal it can be seen as an advantage to be able to track the documents and those who access them (Bennett, 2001).

However, web bugs are now being used for other less wholesome reasons for example, web bugs are regularly placed on websites by online advertising companies. They are placed on websites to collect information on a user's habit. The web bugs gather information on what the person is doing online, like what website's they are visiting and when (Chung & Paynter, 2002).

2.3.3 Spyware

Spyware was first used with only good intentions in mind similar to cookies and web bugs. They were originally created to help users with problems occurring from programs on their machines. If there was a problem with the program, a spyware program would allow a pop up to help the user solve their problem (Barker, 2006). Spyware has now developed into a more sinister tool. In the majority of cases spyware is installed without the user's knowledge or consent. Spyware normally arrives on a person's machine when a user installs a free software program without reading the full licensing agreement. The spyware then proceeds to collect information secretly and forward it on to advertisers or other interested parties (Duke, 2002). A study took place in 2005 to investigate the occurrence of spyware and what information it gathered. The study began by downloading freeware and investigating website's they believed had spyware present. Other findings showed a low occurrence of spyware but still highlighted the inherent dangers of what personal information could be gathered and shared. For example under investigation iMesh[2] was found to have sent a large amount of personal information. Some of the personal information sent was name, country, year of birth, martial status, gender, personal interests, zip code and email. This study highlighted that spyware may not

[2] iMesh is a online social and file sharing network.

be on every website visited but on those where it is present it can gather large amounts of personal information. The study also highlighted the amount of personal information that can be gathered (Kucera et al; 2005). It also shows a need for people to be aware and cautious in relation to spyware. Although spyware was not as widely in use as first believed it still is out there. Spyware is emphasised here as still a problem and people's awareness of this needs to be examined.

2.3.3.1 What spyware does?

Once a machine is infected with spyware its main objective is to gather information from the infected user's machine. Spyware is very effective in getting on to a user's machine in the beginning. The spyware installs itself alongside a legitimate program or download, without any consent being given from the user. In some cases consent is sought from the user, but the majority of these cases an uninformed user may just accept the install without reading it fully. Education of users would help in this matter but the majority of spyware is installed without consent. Some spyware programs have even become so complex that it searches a user's computer for anti-spyware programs and deletes them before installing new spyware (Barker, 2006; Duke, 2002; Shaw 2003).

2.3.3.1.1 Redirect Web Links

Spyware alters websites visited by the user on the infected machine so that the advertising that appears on the page is the advertisements that the spyware wants the user to view. A switch occurs between the two advertisements, the one that should appear and the one the spyware wants to appear. This is an obvious attempt to entice users to a particular website but without paying for the advertising (Barker, 2006; Shaw 2003).

2.3.3.1.2 Changes to user machine

Spyware can affect many changes on a user's personal computer (PC), but two of the most common types of changes are a change to the user's homepage and the changing of a dial up number. The spyware alters the homepage on the user's machine so when the user launches their web browser the spyware homepage opens rather than the user's choice of homepage. In most cases the user can change it back straight away to their original and preferred homepage. However, in some cases the spyware that altered the homepage must be found and deleted before the change of homepage is removed. Another, perhaps more sinister occurrence of alterations to the user's machine is that of dialling a high toll telephone number to connect to the Internet. This type of alteration may not be noticed until the user receives a highly expensive phone bill (Barker, 2006; Davis, 2007; Shaw 2003).

2.3.3.1.3 Key logging

Perhaps the most dangerous and biggest invasion of privacy is a type of spyware called key loggers. This type of spyware monitors the keystrokes of a user on an infected machine. While monitoring the keystrokes of the user, the spyware program records all the information that the user enters, including credit card information, e-mail addresses and online banking information. All this occurs without the knowledge of the user so he/she may not know their user name and password information is being collected until money goes missing from their accounts (Barker, 2006; Forte, 2005; Shaw, 2003).

2.3.3.1.4 Removal of Spyware

Spyware can be extremely difficult to locate and remove from a user's machine once installed. Even with all the software programs available to remove spyware, not one of the software removal options holds all the answers but at least all make strong attempts at blocking key logging spyware. In order to remove spyware completely

from a machine a combination of spyware removal products should be used (Barker, 2006; Davis, 2007).

2.3.4 Summary

There are other methods for the collection of information online but cookies, web bugs and spyware are the most common type. All of these collection methods are worrying in their own unique way. There are steps that can be made to protect your personal information online, which will be discussed later in this chapter.

2.4. Companies' usage of personal information

Once a user's personal information has been collected either via the methods above or in any other way, what happens with this information. Personal information is used like any other asset belonging to the organisation, which can be bought and sold. This information is valuable information for advertising companies or any one else who requires it.

The information that is collected by online companies is valuable and is seen as an asset even if they did not mean to collect that information. There have been several cases of the collection of personal information in error and many papers written on this area (Bennett, 2001). An example of this is a program called Cue Cat that Radio Shack and its manufacturer is Digital Convergence Distributed. The idea behind Cue Cat was straight forward as it did not seem to pose a threat to people's privacy. It worked on a simple principle that when a user was reading a newspaper or magazine online and an advertisement grabbed their attention, Cue Cat would scan the advertisement and bring the user to the relevant website. This simply gave convenience to the user who no longer had to type in the URL. All this seems

simple and straightforward but when installing the information users were asked for their sex, age range, zip code, name and email address. All this information was transported to the Digital Convergence database and each time that Cue Cat was used the database was informed and the information added. This obviously heightened concerns among those worried about their privacy (Bennett, 2001).

Some companies have also tried to use the information as an asset once bankruptcy has occurred. Some examples of these companies are toysmart.com, living.com and voter.com. These companies do not have the assets that non online companies may have, for example, having a property to sell to pay creditors in the bankruptcy process. As the online companies had no tangible assets to sell they listed their intent to sell personal information they had acquired (Carroll, 2002).

These companies never set out with the intent to use people's personal information as an asset, it was merely a consequence of bankruptcy in this case. In some cases however, the use of personal information as an asset is not a consequence but a careful business decision one such organisation to do this is DoubleClick.

2.4.1 DoubleClick

DoubleClick is perhaps the biggest online advertising agency. DoubleClick was founded in New York as an advertising agency that targets its advertisements in a very narrow and focused manner. It achieves this narrow focus by looking at what user's do as they use the Internet. The problem with DoubleClick is they do not only examine what website's a user visits but also look at a user's machine and gather information on the computer's software. DoubleClick then uses all this information to target advertisements at the user for products/services they may wish to buy (Bennett, 2001; Moukheiber, 2006).

DoubleClick don't know exactly who you are per say. They don't know your date of birth, address, telephone number or any other personal information about you. The DoubleClick objective is to build a picture of you and your online activity. Once you enter a website that has a DoubleClick advertisement, DoubleClick will give you an ID number which results in storing the ID number on your computer. The ID number is then used to track your online movements. DoubleClick achieves this through the use of cookies. In the future whenever you visit a site that has a DoubleClick advertisement, DoubleClick may build up a more absolute picture of you (Bennett, 2001; Moukheiber, 2006).

DoubleClick doesn't know who the users are, but are merely aware of their online habits. This all seems innocent enough as they don't know who the person is but movement is still recorded. DoubleClick could take advantage of this by cross referencing your information with another database of information (Moukheiber, 2006). In 1999, DoubleClick made moves to achieve this by purchasing an offline database called Abacus. Abacus collects consumer information from about 90 million homes and 1,800 companies. Once DoubleClick purchased Abacus it had the ability to cross-reference Abacus's name and addresses with DoubleClick's online database (Alster et al, 2000; Bennett, 2001).

DoubleClick received very bad publicity for the move to buy Abacus. There was a drop in share prices and legal action against the company simply from public pressure. DoubleClick agreed to limit how it would link both databases (Alster et al, 2000; Bennett, 2001). This was seen by many as merely a publicity stunt with the very real possibility that behind closed doors the databases are still linked. To help prevent such thinking DoubleClick moved to appoint an advisory board on privacy in 2000. This privacy advisory board was just that – an advisory board that DoubleClick does not have to listen to but merely give the impression it is listening to the advice been given (Wingfield, 2000).

2.4.2 Summary

DoubleClick is just an example of how companies examine what user's do online. Possibly the most worrying aspect of what companies like DoubleClick do is that people are not aware they are doing it. The question then should be, is there anyway for the users to stop them from checking how certain information can be taken without the user's agreement. There are some methods to protect your personal information online and are discussed in the next section.

2.5 Technological Tools to Protect Users Online

There have been many technological developments in order to try to aid people in protecting their privacy online. The main area of development has been the introduction of programs to hide a user's IP address from which they can be tracked down. Some of the main methods developed are onion routing, lucent personalised web assistant, platform for privacy preferences project (P3P) and TRUSTe. Onion routing works by the user submitting an encrypted HTTP request using a series of symmetric cryptographic algorithms and keys to unlock the information that is being transmitted. With lucent personalised web assistant an agent is used as an alias to build a consistent but unidentified relationship with websites (Gritzalis, 2004; Patel & Juric; 2001).

The platform for privacy preferences project (P3P) was developed by the World–Wide-Consortium (W3C)[3] and TRUSTe was developed by a non profit organisation, both are discussed in section 2.5.1 and 2.5.2 (World-Wide-Consortium, 2003; TRUSTe).

[3] W3C develops interoperable technologies to lead the Web to its full potential.

2.5.1 Platform for Privacy Preferences Project (P3P)

P3P was developed by the World-Wide-Consortium (W3C). It was developed to allow user of the Internet reach agreement with any website's privacy with regards to their privacy policy. P3P was developed to allow for a standardised way for website's to display their privacy practices to users who wish to use their website. P3P allows users to access the security policy of a website so it's understood with ease by the user. According to the W3C P3P allows users to interpret the privacy practices of website with ease, allow their computer to make some decisions regarding privacy once the set-up of P3P has been completed and even cater for their relationships with specific websites. The overall goal of the P3P project is to allow users have prefaces over what information website's can gather about them (Gritzalis, 2004; World-Wide-Consortium, 2003).

Therefore, by having P3P enabled website browsers, users can decide upon a website's security policy and how much these polices match what information they wish to give out. P3P is based on an XML scheme to allow vendors to publish their privacy policies in a machine readable format (Gritzalis, 2004; World-Wide-Consortium, 2003). XML is short for Extensible Markup Language. XML was developed by W3C specifically for web documents. A markup language allows a user to process, define and present text in a certain manner (Webopedia.com). The adoption rates of P3P have never reached the levels desired according to a study carried out by Beatty et al, 2007. The study examined 5,553 website's with only 463 website's having P3P, resulting with a percentage of 8.34%. This highlights that a new technology like P3P will take a long time to reach the desired levels of adoption (Beatty et al; 2007).

2.5.1.1 How P3P works?

P3P includes a standard vocabulary for describing what a particular website does with the data it collects and a schema for describing what data they collect. This information is presented in a P3P policy document. The policy document is a compilation of the vocabulary and the data practices of a website. The policy is made up of multiple choice questions so it does not contain as much detail as a human readable privacy policy. As the P3P policy is meant to be read by computers rather than by people, multiple choice questions work better. The format of the P3P policy is standardised so it can be automatically processed by a computer (Cranor, 2002; Gritzalis, 2004; World-Wide-Consortium, 2003).

Within the P3P specification a protocol for requesting and transmitting P3P is included. The P3P protocol uses an extended version of the HTTP protocol that is used for communication between Web browsers and Web servers. The machine of the P3P user sends a HTTP request to gather the P3P policy reference file from a given location on a website. The policy reference file gives out the location of the P3P policy of the website. It also points out if a website has one general policy or different policies for different sections of a website. The user agent then retrieves the policy, examines it and takes steps in accordance with the user's preference (Cranor, 2002; Gritzalis, 2004; World-Wide-Consortium, 2003).

2.5.2 TRUSTe

The TRUSTe seal program's main focus is to protect consumer privacy online. The TRUSTe was founded and developed by the CommerceNet Consortium and the Electronic Frontier Foundation (EFF). Both of these organisations are involved with developing the Internet. The CommerceNet Consortium works to help encourage sales over the Internet. The EFF works to develop free expression, social responsibility of the media that is the Internet and to protect people's privacy online.

The EFF is a non profit organisation. In 1996 the two organisations joined forces and TRUSTe was born in 1996. The purpose of TRUSTe at the time was to encourage the growth of Internet based sales by making the Internet a safer place to do business. The official launch of the TRUSTe privacy seal occurred on June 10, 1997. TRUSTe administers its sell to websites of companies that agree to protect people's personal information online when visiting their website. The rationale behind TRUSTe is that people have a right to visit a website without the disclosure of their personal information without their knowledge (Basile et al, 1998; Gritzalis, 2004; Hall & Larson, 2000; TRUSTe).

2.5.2.1 How TRUSTe works?

The TRUSTe program is based upon a set of principles and a consumer compliant resolution program. To gain the TRUSTe seal an organisation must have an acceptable privacy policy that it agrees to maintain. The organisation must write their own privacy policy as TRUSTe believes that no one generic policy would be suitable for all websites on the Internet. TRUSTe does however have an online wizard to help organisations write their privacy policy. Within the privacy policy there must be a clear definition of how the organisation plans to protect people's personal information. The privacy policy of the organisation must reflect clearly how it gathers and distributes the information gathered on their website. These practices must meet the requirements set by TRUSTe (Basile et al, 1998; Gritzalis, 2004; Hall & Larson, 2000; TRUSTe).

Once an organisation has applied for the TRUSTe trustmark for their website TRUSTe performs an initial review. TRUSTe then carries out regular reviews to ensure the organisation is operating the website as set out in the privacy policy and possible improvements that can be made are identified. These reviews can even include an audit of the website's records. This procedure can take a long time to work through to insure that a person's personal information is protected. Once

TRUSTe feels that the website has meet the necessary criteria then the TRUSTe trustmark can be issued (Basile et al, 1998; Gritzalis, 2004; Hall & Larson, 2000; TRUSTe).

TRUSTe then carries out regular reviews of the website to insure they are sticking to the privacy policy that they set out. These reviews are carried out in two main ways by performing compliance reviews and encouraging users of the website to report violations (Hall & Larson, 2000; TRUSTe). The compliance reviews are completed by visiting the websites that have been given the TRUSTe trustmark. Any breaches that are noted are then investigated fully. If upon investigation the website is found to be in breach of their privacy policy, TRUSTe may cancel their trustmark (Hall & Larson, 2000; TRUSTe).

If a user feels a website has breached its privacy policy it can report this fact to TRUSTe. Within the TRUSTe program it is required that the user who feels aggrieved must first attempt to fix the problem with the website. If the user then feels they have been dealt with incorrectly a complaint can then be registered with TRUSTe. TRUSTe then acts as a third party moderator between the user and the website. If the website does not respond in an effective and efficient manner a full review may be carried out (Hall & Larson, 2000; TRUSTe).

2.6 Summary Literature Review

As shown in this chapter, privacy is a major concern for those who use the Internet on a regular bases. A review of the literature shows that individuals are still not fully aware of the consequences of disclosing personal information when using the Internet.

This study will further investigate the awareness of individual's knowledge of software that can invade their privacy online. At this point it is appropriate to confirm the research objectives of the study,

Research Objective:

To measure the target population awareness levels of Internet privacy and possible software and tools used by companies to gather their personal information online.

- Which is more important convenience or privacy in term of male and female users

- Are there different levels of awareness of possible threats to online privacy dependent on the student's background area of study

2.7 Conclusion

This chapter began with a brief overview of the history of the Internet along with some explanations of some common terms that may be used when a discussion on the Internet takes place. The chapter highlighted three common tools used to infiltrate the privacy of Internet users; these were cookies, web bugs and spyware. In each case an explanation of what they can do was provided. Cookies can invade a user's privacy online by tracking websites and links visited as well as monitoring when a user is logged on to a website or not. Web bugs collect information on when and what web sites a user visits. Spyware can threaten a user's privacy by collecting their username and password by using key loggers. A Harris interactive survey in (2000) as cited by Bennett (2001), found that 56 per cent of adults who responded were very concerned about a loss of personal privacy. The loss of personal privacy was rated above topics such as crime.

This was followed by a description of the usage by one company, DoubleClick, of what they do with the information gathered. Possible methods for users to protect themselves online were then reviewed.

Following on from the information gathered in the review of the literature the research objectives for this study were developed. As the most common tools for the invasion of personal privacy online are cookies, web bugs and spyware, the main objective of this study will measure the target population's knowledge of these tools. As shown by previous studies the loss of personal privacy is a cause for high levels of concern so this study will investigate if it is rated higher than convenience among the target group. The differences among male and female respondents will also be investigated as part of the research objective to see if this has any relation with levels of awareness. Also the target group will be investigated further for their level of awareness and knowledge of cookies, web bugs and spyware, based on their area of study, i.e., business, engineering, science or humanities. The remaining chapters

will include details on how the research was carried out and the findings that arose from it.

Chapter Three:

Research and Methodology

3.1 Introduction

The selection of the most appropriate research methodology is vital in order to obtain the most accurate results from the research objectives of this project. Therefore, this chapter will look into the various methods available and examine in more detail the methodology that was chosen. To begin with there is a discussion regarding data types and methods of collection. Subsequently the discussion of the research and sub research objectives are discussed, ultimately leading to the choice of what deemed most suitable. Finally, there will be a brief overview of the various data sources available.

3.2 Data Types/ Methods

"Data collection is crucial to all research. Through this process, researchers accumulate empirical material on which to base their research" (Ibert et al, 2001). It depends on the characteristics of the research whether the researcher adopts a quantitative or qualitative approach for their data collection methods (Ibert et al, 2001).

3.2.1 Qualitative Vs Quantitative research

Qualitative and quantitative are often used to divide the methods of investigation by a researcher into those that are concerned with obtaining an insight and an understanding of the task at hand; qualitative research, and those that are often used to measure things; quantitative methods (Hague, 2002).

Qualitative research is often used to describe any data collection techniques that will generate or utilise non-numerical data, and may even refer to non-verbal data like

video clips or pictures (Saunders et al, 2007). Bannister et al (1994), as cited by Webb (2002), summarise the area eloquently as they write:

> "Qualitative research is:
>
> a) an attempt to capture the sense that lies within and that structures what we say about what we do;
> b) an exploration, elaboration and systemisation of the significance of an identifiable phenomenon;
> c) the illuminative representation of the meaning of a delimited issue or problem."

Qualitative research is often used in place of quantitative data collection when the researcher is less interested in the amounts or percentages of how people do certain things but is more interested in the whys and wherefores (Proctor, 2003). According to Webb (2000) the main reason for this is, qualitative research can be used 'to investigate respondents' beliefs, feelings and attitudes in a way which may not be possible, or not nearly so effective, if they were to be asked to respond to direct questioning'. Qualitative research can take numerous forms, these include; focus groups, observation, in-depth interviews and projective interviewing techniques (Webb, 2002; Hague, 2002).

Quantitative research is at the opposite end of the spectrum and is involved in any data collection or analysis techniques that generate and/or uses numerical data (Saunders et al, 2007). Quantitative research is more focused on the generation of numbers and percentages. As a result, it is often used to measure awareness of an item or opinions that people hold towards a product or whatever it is the research is being carried out on (Proctor, 2003). The type of data generated from quantitative research can vary from counts, to test scores or frequency of occurrences (Saunders et al, 2007). Quantitative research, like its counterpart, also has many forms, the most prominent being questionnaires or surveys. Others include structured interviews, audits and censuses (Hague, 2002; Proctor, 2003).

Quantitative and qualitative research each have there own negative and positive arguments to conduct a study. Qualitative research is more concerned with a detailed examination of the why rather than the how. Quantitative research on the other hand is more concerned with the percentages and the how something is done. In the case of this study a quantitative approach was deemed to be most suitable as quantitative studies are most effective in the measurement of awareness levels, which is what this study to trying to achieve.

3.3 Research Approaches

Research approaches have different strengths and weaknesses and they are more or less applicable in different situations. The research approaches that were looked at for this study include, action research, survey, ethnography and field research.

3.3.1 Action research

Action research has been in use in the social and medical sciences since the mid twentieth century. Action researchers believe the best way to learn about a phenomenon is to experience it first hand (Easterby-Smith et al, 1997). If, once their study is complete, the researcher feels no change is required they must be able to explain why, supporting any claims with evidence. Should the study not be at the level required the researcher must take action to improve it and assess the impact any changes will have (McNiff & Whitehead, 2002).

In order to complete action research in an effective manner the researcher must have a close relationship and a high level of understanding of the phenomenon they are researching. As a result there are problems with action research. These include

issues about time and inevitably the personal understanding of the researcher, which will invade the recording of the information (McNiff & Whitehead, 2002).

After examining action research it was decided that it was not a good option for the carrying out of this study as it is more suited to studies in the medical and social sciences. Also the amount of time needed to complete action research was not available to the researcher.

3.3.2 Ethnography

Ethnographic research requires a researcher to immerse themselves in the natural setting of the phenomenon being observed over a long period of time. This allows the researcher to gather first hand key data about the phenomenon being studied (Vidich & Lyman, 1994).

Ethnography research is most appropriate when the area of the phenomenon being studied is in fact part of a complex social situation. The researcher must closely observe and engage in the everyday activities and document these in detail (Vidich & Lyman, 1994).

After careful consideration it was determined that in order to carry out ethnography research to a high standard and gain good results, the study would not be completed with the time constraints involved.

3.3.3 Field Research

Field research is a methodology often used to challenge current theories and their underlying assumptions. It requires the researcher to process and arrange large amounts of data from multiple sites in order to answer a research question (Miller,

1991). The research is conducted in an assimilation where the environment the phenomenon is most likely to or would occur in. This type of research requires the researcher to carry out very close observations. Field research is not favoured by some researchers as the levels of control they can exercise over the situation are limited. However, it should be noted that studying a phenomenon in this way can be a better way than in laboratory settings (Kent, 1999).

As this study was aiming to measure people's awareness of Internet privacy it was decided that field research would not be suitable in order to gain the desired results.

3.3.4 Survey

Surveys are generally labelled as either personal, telephone or postal according to the method of communication that is used. Virtually all postal surveys, a large majority of telephone interviews or some personal interviews are structured interviews. While, techniques such as in-depth interviews and focus group interviews would usually be unstructured in nature (Brannick & Roche, 1997). Many people are of the opinion that surveys and questionnaires are the same thing when in fact questionnaires, interviews and observations are methods used to carry out surveys (Oates, 2006).

Due to time constraints and nature of this study, surveys would not be a viable option in order to gain the desired results.

3.4 Data Sources

The section below discusses different forms of gathering data. Following this the research area for this study is given with detail on appropriate research approach chosen. At the end of this section a decision will have been reached as to which will give the best results in this study.

3.4.1 Personal Interviews

A personal interview is defined by Cooper and Schindler (1998) as a "two-way conservation initiated by an interviewer to obtain information from a respondent". There are three approaches that are the most common for the collection of data with this method. These are informal conversational interview, standardised open-ended interview with open-ended questions and general interview guide. Informal conversational interviews are very quickly adaptable to individual situations as there are no preset questions. Standardised open-ended interviews are different to informal conversational interviews as each person interviewed is asked the same questions. Open-ended questions are written to give the interviewee an opportunity to respond freely and state answers that go further than a simple "yes" or "no". The general interview guide is effective when information from different areas must be obtained (Patton, 2002; Kent 1999).

These types of interviews have some key advantages as stated by Kent (1999):

- The eligibility of the participant to partake in the interview can be checked before the interview begins
- If a questionnaire is to be followed the interviewer can ensure questions are asked in correct order and all relevant questions are put to the respondent

- The interviewer can insure questions are understood fully and can encourage full and comprehensive answers from the interviewee
- Response rates are much higher than with other research methods

Personal interviews were not used to carry out this study as they are too time consuming in relation to the constraints of this study.

3.4.2 Questionnaires

Questionnaires have been a method of conducting research since the 1970's. Questionnaires are often used in conjunction with interviews as a guide to collecting data but they can also be used as an independent method of data collection. Kent (1999) defined a questionnaire "as any document is an instrument with which to capture data generated by asking people questions". So in theory a questionnaire is a set of questions to withdraw the desired data from the respondent. The construction of the questionnaire can be broken into four intertwined areas; preliminary considerations, asking of questions, construction of the questionnaire and pre-testing the questionnaire (Kent, 1999; Proctor, 2003).

3.4.2.1. Preliminary Considerations

According to Proctor (2003) a researcher must translate their research problem into a series of research questions before the questions for the questionnaire are developed. The research questions should identify:

- What information is required?
- Who are the target respondents?
- What type of data collection method will be used?

In chapter 2, the literature in Internet privacy was reviewed which lead this study to develop a research objective. This showed the research problem area which will be mentioned in section 3.5.

3.4.2.2 Asking of the questions

Each question that is placed on the questionnaire must meet a set of criteria. Proctor (2003) set out a number of considerations:

- Know the reason for asking each and every question
- The questions must be set out in a clear manner
- Language that is familiar and natural should be used
- Avoid double-barrelled questions
- If giving alternatives they should be stated clearly
- Questions should be reliable and valid

3.4.2.3 Construction of the Questionnaire

In order to successfully construct a questionnaire some key points made by Proctor (2003) will aid the researcher:

- Know when to use open-ended in contrast to closed-ended questions
- Know the appropriate number of response categories and their description in the case of closed-ended questions
- Ensuring a free movement through the questionnaire from evaluative to diagnostic to classification type questions.

3.5 Research Area

In chapter 2, the review of the literature showed that privacy was a serious issue and rated above crime by 56 per cent of adults who responded to a Harris interactive survey in (2000) as cited by Bennett (2001). Also highlighted, in the review of the literature was the need to investigate people's perception on Internet privacy, their awareness of what technological tools could invade their privacy online and how these tools collect and store their information (Bennett, 2001; Dasgupta & Turner, 2003; Graeff & Harmon, 2002; Kucera et al, 2005). While examining the different possible ways to carry out the research it was necessary to first of all identify the research and sub research objectives. These are as follows,

- To measure the target population awareness levels of Internet privacy and possible software and tools used by companies to gather their personal information online.

    - Which is more important convenience or privacy in term of male and female users

    - Are there different levels of awareness of possible threats to online privacy dependent on the student's area of study

This study will measure college student's view of their privacy online. College students were chosen as the target population for many reasons. The majority of current college students are from a generation of Internet users who have grown up using the Internet and feel comfortable using the Internet to carry out everyday tasks. College students were also chosen as they were very accessible for the researcher. The college students in this study comprise of 43.59 per cent of female students and 51.41 per cent of male students.

3.6 Appropriate Research Approach

This study examines college student's knowledge of possible threats to their online privacy. Threats to online security come in many ways but the main focus of this study will be on software threats. The main focus will be on "cookies", "web bugs" and "spyware". Each of these pieces of software were originally developed as tools to aid those who use the Internet and are now threats to security (Baker 2006; Bennett, 2001; Beise et al, 2001; Chung & Paynter, 2002; Cunningham, 2002; Dasgupta & Turner; 2003).

Once all the available research options were studied it was decided that due to the constraints on the study and the numbers of respondents required a quantitative questionnaire would best suit this study. A questionnaire was chosen as it can be circulated easily to a large number of participants in a short space of time. It is also the best to approach to carry out an analysis on a large number of questionnaires in an efficient and effective manner. Using Proctor (2003) guidelines this questionnaire used closed-ended questions. A limited number of response categories were given. The language in the questionnaire was straight forward and easy to understand. The questionnaire was planned so that the reader could clearly understand that section I related to background information, section II related to Internet usage and section III related to the readers knowledge of possible software tools to invade privacy online.

3.7 Conclusion

This chapter highlighted various research options available to the researcher in order to meet the research objectives. The chapter justifies the choice of a quantitative approach in conjunction with a questionnaire. At the end of the chapter a thorough description of steps that can be taken to ensure the questionnaire developed pertains to a high standard. This questionnaire will gather data to analyse people's knowledge and views of online privacy. The remaining chapters will present the results of this analysis, draw conclusions and finally, possible further research will be discussed.

Chapter Four:

Discussion of Findings

4.1 Introduction

The chapter will outline the findings of this study. Quantitative research using questionnaires was applied in this study. The purpose of using questionnaires with closed-ended questions was to measure awareness of the target population's view on Internet privacy and the possible threats to their privacy online. The beginning section discusses the results of the questionnaire focusing on each set of questions. In the second section of this chapter the results of the questionnaire with relation to the research objectives will be discussed. This research analyses the results of a questionnaire on seventy people. The target population for this study were college students as they are easily accessible and from a generation of people who are comfortable with Internet usage.

4.2 Questionnaire Results

The questions on the first section of the questionnaire were asked in order to gauge the demographic of those who answered the questionnaire. This was not a direct objective of the study but necessary in order to gain a full picture of those who filled in the questionnaire.

Table 4.1 Sex of respondents

"Respondent's Sex"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	43	61.4	61.4	61.4
	Female	27	38.6	38.6	100.0
	Total	70	100.0	100.0	

The breakdown of the gender of the students surveyed is not equal as 61.4 per cent of those who took part were male and the remaining 38.6 per cent female. This is not

completely indicative of the population of the college with 48.59 per cent of the college population being female and 51.41 per cent being male.

Table 4.2 Age of respondents

"In what age group do you fall?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	17-19	17	24.3	24.3	24.3
	20-22	24	34.3	34.3	58.6
	23-25	17	24.3	24.3	82.9
	26-29	4	5.7	5.7	88.6
	30-35	3	4.3	4.3	92.9
	36-44	2	2.9	2.9	95.7
	45-54	1	1.4	1.4	97.1
	55 +	2	2.9	2.9	100.0
	Total	70	100.0	100.0	

The majority of the students fall into the first three age categories of 17-19, 20-22 and 23-25 with 24.3 per cent, 34.3 per cent and 24.3 per cent respectively. This represents a cumulative percentage of 82.9. The division of the population into the age categories was expected to follow this pattern of unequal distribution, as the perceived college going age in Ireland falls neatly between the ages of 17 and 24.

The following questions were asked to gain an understanding of the education level of those who were questioned and also how long then had been using computers. It was important to know how long those questioned on average had been using computers.

Table 4.3 Level of education

"Please select the level of education you have completed"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Secondary education or equivalent	28	40.0	40.0	40.0
	Third level education or equivalent	41	58.6	58.6	98.6
	5	1	1.4	1.4	100.0
	Total	70	100.0	100.0	

This table highlights that 58.6 per cent of those questioned have completed some third level education with an additional 40 per cent having completed second level education.

Table 4.4 Length of time using computers

"How long have you been using computers?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	<6 mths	2	2.9	2.9	2.9
	1-3 yrs	4	5.7	5.7	8.6
	4-6 yrs	23	32.9	32.9	41.4
	7 yrs +	41	58.6	58.6	100.0
	Total	70	100.0	100.0	

Almost all (91.5 per cent) of those questioned have been using computers for four or more years. With many 58.6 per cent (of the total) using computer for over seven years. This was expected by the researcher as the generation is known as Generation T, where the T stands for Technology.

An even amount of questionnaires were disseminated to four schools within the college and 70 questionnaires were returned in all. As table 4.3 shows, 22 were received from the school of engineering, 21 from the school of business, 16 from the school of science and 11 from the school of humanities.

Table 4.5 Study area of respondents

"I am a student of the school of . . ."

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Engineering	22	31.4	31.4	31.4
	Business	21	30.0	30.0	61.4
	Information Technology	16	22.9	22.9	84.3
	Humanities	11	15.7	15.7	100.0
	Total	70	100.0	100.0	

The percentage of those from each school questioned is not indicative of those currently registered in full time courses. With 25.34 per cent registered in humanities courses and only 15.7 per cent of those questioned representing the humanities area. There were two schools not involved in the questionnaire these were education and health sciences.

The questions within the second section of this questionnaire were asked to examine the participant's usage of the Internet and other possible locations to monitor if they had control over their Internet settings. This was essential if there were people aware of threats as they could then alter their settings to protect themselves or in another case have someone else looking after their privacy needs.

Table 4.6 Do respondents use the Internet in WIT.

"Do you use the Internet in WIT?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	70	100.0	100.0	100.0

Expectedly all of those questioned do avail of the Internet within WIT. It should be noted that within the college the security settings of the Internet browser are preset and students are unable to alter this in any way. Also it appears necessary to note here that the Internet is free to students of the college and as a result may entice

those who are either unwilling or unable to pay for such a service to take advantage of it.

Table 4.7 Other locations respondents use Internet

"In what other locations do you use the Internet?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Home	62	88.6	89.9	89.9
	Internet cafe	3	4.3	4.3	94.2
	Personal Digital Assistant (PDA) Wireless	4	5.7	5.8	100.0
	Total	69	98.6	100.0	
Missing	System	1	1.4		
Total		70	100.0		

The results here show that almost 90 per cent of those questioned use the internet in the home. This is higher than was expected as it was assumed by the researcher that many of those questioned would be living in rented accommodation. It was thought that the use of the Internet in the home would be minimised as a result because frequently this is an amenity not present in many rented houses or flats. The other results here were expected however, as PDA's are essentially aimed at business people who are on the move a lot more than students would be. Also it was expected that students would be less likely to pay for online use in Internet café's when the service is available free of charge within the college campus.

These two questions were asked to find out how long people have been using the Internet and how many hours per week they spend on the Internet. These were important so a picture could be built up on how often and for how long people are prone to threats to their privacy.

Table 4.8 Length of time using the Internet

"How long have you been using the Internet?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	<6 mths	3	4.3	4.3	4.3
	1-3 yrs	9	12.9	12.9	17.1
	4-6 yrs	32	45.7	45.7	62.9
	7 yrs +	26	37.1	37.1	100.0
	Total	70	100.0	100.0	

These results were as expected in this category as the numbers of Internet users in general has risen greatly over the past decade. Perhaps the most surprising results from this table is that 4.3 per cent of those questioned have only been using the Internet for less than 6 months.

Table 4.9 Average hours per week spent on Internet

"On average how many hours a week do you spend on the Internet?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-1 hrs	3	4.3	4.3	4.3
	2-4 hrs	18	25.7	25.7	30.0
	5-6 hrs	10	14.3	14.3	44.3
	7-9 hrs	19	27.1	27.1	71.4
	10-20 hrs	12	17.1	17.1	88.6
	21-40 hrs	7	10.0	10.0	98.6
	40 hrs +	1	1.4	1.4	100.0
	Total	70	100.0	100.0	

These results are a little surprising as they are not as the researcher assumed they would be. The initial expectation was that the majority of the students questioned would spend between 10 and 20 hours per week on the Internet when in reality only 17.1 per cent of those questioned fell into this usage category. Just over a quarter (27.1 per cent) of the students claimed to use the Internet for a period of seven to nine hours every week. But most surprisingly a further 25.7 per cent admitted to using the Internet for a maximum of four hours in a week.

These next three questions were asked in order to find out whether or not people have ever been requested to supply personal information online and if a company's reputation had any influence over whether or not they supplied the requested information. The final question in this sequence was asked to see if people would provide personal information if they received compensation. It was important to see if people were asked for personal information in an open manner or was it all collected in a more secretive way.

The second element of section two on the questionnaire were questions to discover if the participants had ever been requested for personal information online. If they had been requested to provide personal information had the offer of compensation or the reputation of the company affected their decision.

Table 4.10 Requested to provide personal information online

"Have you ever been requested to provide personal information when visiting a website?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	51	72.9	72.9	72.9
	No	18	25.7	25.7	98.6
	3	1	1.4	1.4	100.0
	Total	70	100.0	100.0	

This result was as expected with 72.9 per cent of those questioned were asked to provide personal information on many Web Sites. This involved the user's registering in order to fully use all of a Web Sites services.

Table 4.11 Is a company's reputation important when providing personal information

"The reputation of a company is important to you when providing personal information online"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	31	44.3	56.4	56.4
	Agree	18	25.7	32.7	89.1
	Disagree	5	7.1	9.1	98.2
	Strongly Disagree	1	1.4	1.8	100.0
	Total	55	78.6	100.0	
Missing	System	15	21.4		
Total		70	100.0		

The results for this question were as expected by the researcher. It was assumed that a company's reputation would be a major factor in a person's decision to part with personal information and with an astonishing 89.1 per cent of the respondents agreeing with the statement that, "The reputation of a company is important to you when providing personal information online".

Table 4.12 Would compensation affect decision to give personal information to a website

"I would be more likely to give personal information to a web site if I were to be compensated in some way"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	9	12.9	16.7	16.7
	Agree	16	22.9	29.6	46.3
	Disagree	26	37.1	48.1	94.4
	Strongly Disagree	3	4.3	5.6	100.0
	Total	54	77.1	100.0	
Missing	System	16	22.9		
Total		70	100.0		

Here it can be seen that over half of the respondent's either disagreed or strongly disagreed with the idea that they would be more likely to part with personal information if they were to be compensated for it in some way. This was unexpected as the researcher thought compensation would be an incentive to these Internet users.

The following nine questions were asked to find out how users use the Internet in a range of everyday tasks. What people choose to do online will affect the exposure that they have with possible threats of their privacy.

Table 4.13 Do respondents use Internet for personal non educational use

"Do you use the Internet for personal non-educational use?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	67	95.7	95.7	95.7
	No	3	4.3	4.3	100.0
	Total	70	100.0	100.0	

Almost all (95.7 per cent) of the students who took part in the survey use the Internet for personal use as was expected by the researcher. This is because the Internet has obvious scope and numerous uses for these individuals.

Table 4.14 Do respondents use the Internet to buy goods

"Do you use the Internet to buy goods?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	49	70.0	73.1	73.1
	No	18	25.7	26.9	100.0
	Total	67	95.7	100.0	
Missing	System	3	4.3		
Total		70	100.0		

The use of the Internet by these students to purchase products was expected to be higher than the 73.1 per cent that do. It was thought that increased security would

have encouraged the use of the Internet as an alternative to the physical shopping process and may have even offered more convenience and more value for money.

Table 4.15 Do respondents use the Internet to pay bills

"Do you use the Internet to pay bills?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	25	35.7	37.3	37.3
	No	42	60.0	62.7	100.0
	Total	67	95.7	100.0	
Missing	System	3	4.3		
Total		70	100.0		

Due to the age of the respondent's, whereby the majority are aged between 17 and 25, it has not been surprising that only 37.3 per cent of those questioned use the Internet to pay bills online.

Table 4.16 Do respondents use the Internet to listen to the radio

"Do you use the Internet to listen to the radio?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	28	40.0	41.8	41.8
	No	39	55.7	58.2	100.0
	Total	67	95.7	100.0	
Missing	System	3	4.3		
Total		70	100.0		

Only a mere 41.8 per cent of the students questioned listen to the radio online. It was anticipated that the Internet would be used by many more of the students for this purpose.

Table 4.17 Do respondents use the Internet to download music

"Do you use the Internet to download music?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	49	70.0	73.1	73.1
	No	18	25.7	26.9	100.0
	Total	67	95.7	100.0	
Missing	System	3	4.3		
Total		70	100.0		

Of those questioned in this survey, 73.1 per cent download music from the Internet. This was lower than was expected. The researcher thought that, with the obvious proliferation of MP3 players and especially iTunes, people, particularly computer users would be more likely to download music.

Table 4.18 Do respondents use the Internet to watch movies

"Do you use the Internet to watch movies?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	41	58.6	61.2	61.2
	No	26	37.1	38.8	100.0
	Total	67	95.7	100.0	
Missing	System	3	4.3		
Total		70	100.0		

Once again this result corresponds to the preconceptions of the researcher. It was thought that some people would use the Internet to watch movies but not as many as would download music. This is because of the excessive time period that is often involved with the viewing of movies online.

Table 4.19 Do respondents use the Internet for general browsing/surfing

"Do you use the Internet for general browsing/surfing?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	67	95.7	100.0	100.0
Missing	System	3	4.3		
Total		70	100.0		

Expectedly, every person questioned uses the Internet for general browsing.

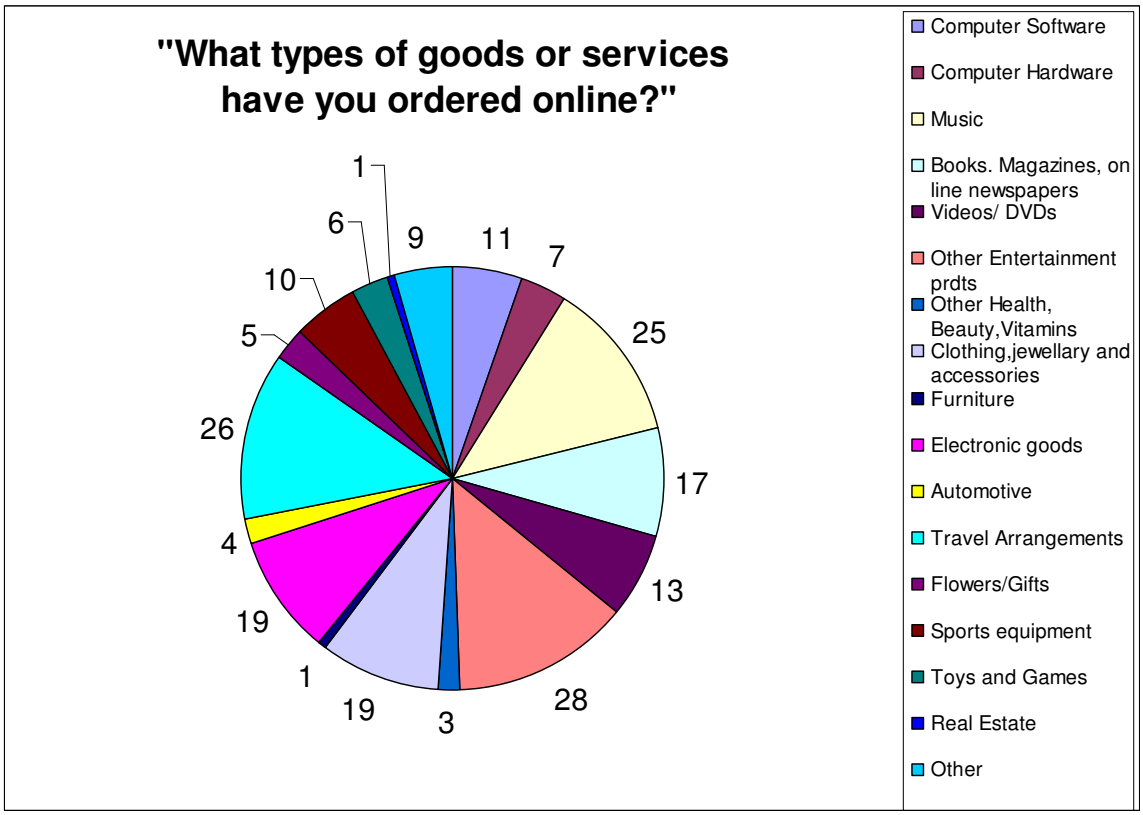
Table 4.20 Have respondents used Internet to order goods or services

"During the last 2 years have you ordered goods or services over the Internet?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	56	80.0	80.0	80.0
	No	14	20.0	20.0	100.0
	Total	70	100.0	100.0	

Although at 80 per cent, a large amount of the respondents have bought goods/services online within the last two years, it was thought that even more people would have bought products in this way.

Table 4.21 What types of goods and services have been ordered online



The types of goods and services ordered online were as expected with 28 of those questioned purchased entertainment products while 26 of the respondents made travel arrangements and 25 people purchased music. This highlights an interesting phenomenon online as 49 people when questioned said they downloaded music but only 25 people stated they purchased it. Perhaps most surprising are the numbers of those who purchased computer software and hardware was only 11 and 7 respectively with this expected to be higher.

Table 4.22 How often do respondents make online purchases

"On average, how often do you make online purchases from Web-based vendors?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Don't buy online	9	12.9	14.5	14.5
	< once a month	31	44.3	50.0	64.5
	About once a month	13	18.6	21.0	85.5
	Several times each month	2	2.9	3.2	88.7
	About once a week	1	1.4	1.6	90.3
	Other	6	8.6	9.7	100.0
	Total	62	88.6	100.0	
Missing	System	8	11.4		
Total		70	100.0		

In the above table it can be seen that half the respondent's make online purchases less than once a month. It was expected that the highest proportion of the students would make purchases less than once a month. It was assumed, however, that the gap between that and the next option of about once a month would be smaller than that apparent here. Also, it was unanticipated that 14.5 per cent never buy products online.

The next two questions were asked in order to see which is more important convenience or privacy. The participants were also asked was privacy important to them.

Table 4.23 Which is important convenience or privacy

"In general which is more important to you?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Convenience	34	48.6	48.6	48.6
	Privacy	36	51.4	51.4	100.0
	Total	70	100.0	100.0	

Surprisingly, almost half of the people questioned in the survey believe that convenience is more important than privacy when using the Internet. This is worrying as there are many sites on the Internet that are simply not as reputable as one would hope and unfortunately these are often the more convenient.

Table 4.24 Is privacy a major concern when using the Internet

"Privacy is a major concern when using the Internet"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	22	31.4	31.9	31.9
	Agree	42	60.0	60.9	92.8
	Disagree	5	7.1	7.2	100.0
	Total	69	98.6	100.0	
Missing	System	1	1.4		
Total		70	100.0		

The results in table 4.24 show that privacy is a major concern when surfing the Internet with 92.8 per cent of the respondents either agree or strongly agree that privacy is a major concern for them when surfing the Internet. This was expected to some degree but it was also thought that more people would have stronger feelings about this, but only 31.9 per cent expressed these strong feelings. The results shown in Table 4.23 do show a conflict of interest between the sets of answers in Table 4.24. People agree that privacy is a major concern but yet convenience is more important.

4.3 Research Objectives

In this section of the chapter the results of the questionnaire in relation to the research objectives will be discussed.

4.3.1 Research Objective

The main research objective of this study was to measure the awareness of software and tools used to gather personal information online among the target population. The respondents through the questionnaire were asked a series of questions to investigate their knowledge of cookies, spyware and web bugs.

The following series of questions were asked in order to determine the respondent's familiarity of cookies.

Table 4.25 Have respondents every heard of "cookies"

"Have you ever heard of "cookies" with relation to computing?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	44	62.9	64.7	64.7
	No	24	34.3	35.3	100.0
	Total	68	97.1	100.0	
Missing	System	2	2.9		
Total		70	100.0		

As "cookies" are probably the most familiar online tracking and information gathering devices it was expected that the majority of students would be aware of these. This was proven as it can be seen here that 64.7 per cent of the students are aware of their existence.

Table 4.26 What "cookie" policy do respondents use

"Which of the following "cookies" policies do you primarily use when browsing?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always accpet	7	10.0	15.2	15.2
	Only accept from the same site I am browsing	10	14.3	21.7	37.0
	Warned before accepting cookies	10	14.3	21.7	58.7
	Ignore/never accept cookies	5	7.1	10.9	69.6
	Don't know what a cookie is	7	10.0	15.2	84.8
	Don't know what my preferences are set to	7	10.0	15.2	100.0
	Total	46	65.7	100.0	
Missing	System	24	34.3		
Total		70	100.0		

The results shown in table 4.26 shows the policies the participants deploy in relation to cookies when browsing the Internet. The results of this table were expected to a degree. However, one result that was surprising is that 21.7 per cent of those surveyed were warned before they accept "cookies". This was unexpected as this is a higher level of security than would be the anticipated norm.

Table 4.27 How often do respondents delete their "cookies"

"How often do you delete your "cookies"?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Every time the Internet is used	8	11.4	17.8	17.8
	Once a day	1	1.4	2.2	20.0
	Once a week	8	11.4	17.8	37.8
	Every two weeks	4	5.7	8.9	46.7
	Once a month	4	5.7	8.9	55.6
	Less frequently than once a month	6	8.6	13.3	68.9
	Never	14	20.0	31.1	100.0
	Total	45	64.3	100.0	
Missing	System	25	35.7		
Total		70	100.0		

The results here are possibly amongst the most surprising of all. It was thought that the majority of the respondents would delete "cookies" regularly, approximately once a week. This showed up to be at just 17.8 per cent. Meanwhile, the same percentage of students delete "cookies" each time they use the Internet, this level of security was not envisaged. Most worryingly of all the results is that almost one third (31.1 per cent) of the students never delete their "cookies".

Table 4.28 Are respondents aware "cookies" can track web sites visited

"Are you aware that "cookies" can track web sites visited?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	30	42.9	63.8	63.8
	No	17	24.3	36.2	100.0
	Total	47	67.1	100.0	
Missing	System	23	32.9		
Total		70	100.0		

Table 4.29 Are respondents aware "cookies" can track links on web sites visited

"Are you aware that "cookies" can track links on individual web sites visited?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	28	40.0	59.6	59.6
	No	19	27.1	40.4	100.0
	Total	47	67.1	100.0	
Missing	System	23	32.9		
Total		70	100.0		

Table 4.30 Are respondents aware "cookies" can monitor if logged onto website or not

"Are you aware that "cookies" can monitor whether you are logged into a website or not?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	24	34.3	51.1	51.1
	No	23	32.9	48.9	100.0
	Total	47	67.1	100.0	
Missing	System	23	32.9		
Total		70	100.0		

Again, because "cookies" are the most common and well known tracking device it was expected that the majority of people would be aware of what they are employed for. This was proven as 63.8 per cent know that "cookies" track Web Site visited, 59.6 per cent are aware that links on individual Web Sites may be monitored and finally 51.1 per cent are aware that "cookies" can monitor whether or not you are logged onto a website or not.

Table 4.31 Are respondents aware "cookies" can identify habits when using the Internet

"Are you aware that "cookies" can identify your habits when using the Internet?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	24	34.3	51.1	51.1
	No	23	32.9	48.9	100.0
	Total	47	67.1	100.0	
Missing	System	23	32.9		
Total		70	100.0		

The result that is shown here is a little worrying as it was expected that more of the respondents would be aware of the use of cookie to track an individuals Internet usage habits.

The following series of question were asked in order to determine the respondent's familiarity of web bugs.

Table 4.32 Are respondents aware of "web bugs"

"Are you aware of what "web bugs" are in relation to computing?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	34	48.6	49.3	49.3
	No	35	50.0	50.7	100.0
	Total	69	98.6	100.0	
Missing	System	1	1.4		
Total		70	100.0		

"Web bugs" are not as common as "cookies" and as a result it is not surprising that just under half of the respondents, 49 per cent, are aware of what they are.

Table 4.33 Have respondents every heard of "web bugs"

"Are you aware that "web bugs" are placed on web site's to collect information on your online habits?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	29	41.4	69.0	69.0
	No	13	18.6	31.0	100.0
	Total	42	60.0	100.0	
Missing	System	28	40.0		
Total		70	100.0		

Table 4.34 Are respondents aware "web bugs" can gather information on what then are doing online

"Are you aware that "web bugs" gather information on what you are doing online for example what websites you visit and when?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	25	35.7	61.0	61.0
	No	16	22.9	39.0	100.0
	Total	41	58.6	100.0	
Missing	System	29	41.4		
Total		70	100.0		

Of those respondents who were aware of their existence, 69 or 61 per cent of those questioned were aware that "web bugs" are placed on web sites to collect information on your online habits and that they gather information on what you are doing online respectively. This result was expected to be as high as this.

The following series of question were asked in order to determine the respondent's familiarity of spyware.

Table 4.35 Have respondents every heard of "spyware"

"Are you aware of what "spyware" is in terms of computing?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	47	67.1	68.1	68.1
	No	22	31.4	31.9	100.0
	Total	69	98.6	100.0	
Missing	System	1	1.4		
Total		70	100.0		

Although this percentage is quite high at 68.1 per cent, it was expected to be even a fraction higher as "spyware" is quite a common form of Internet tracking and information gathering.

Table 4.36 Are respondents aware of the most likely way to get "spyware"

"Are you aware that the most likely way to get "spyware" on your computer is by downloading freeware?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	31	44.3	59.6	59.6
	No	21	30.0	40.4	100.0
	Total	52	74.3	100.0	
Missing	System	18	25.7		
Total		70	100.0		

The results in table 4.36 are a little surprising as it was believed that a larger percentage of people are aware that by downloading freeware one is more likely to encounter and download "spyware". This was expected because "spyware" is a very familiar tracking tool.

Table 4.37 Are respondents aware of the type of "spyware" called key loggers

'Did you know that a type of "spyware" called key loggers can track all your usernames and passwords while you are online?"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	20	28.6	38.5	38.5
	No	32	45.7	61.5	100.0
	Total	52	74.3	100.0	
Missing	System	18	25.7		
Total		70	100.0		

This result is somewhat worrying as it was expected that a lot more than 38.5 per cent of the respondents would be aware that "spyware" is capable of tracking both a person's username and their password when they are logging into Web Sites.

Overall the awareness levels of the target population on software and tools that can invade there privacy online was as expected. With the highest awareness levels being with cookies followed by spyware and then web bugs. This was as expected as cookies are the most common tool in use and web bugs being a newer technology.

4.3.2 Sub Research Objective One

The first sub research objective was to investigate any possible difference of opinion between male and female Internet users in relation to convenience and privacy.

Table 4.38 Which is more important to respondent's convenience or privacy

"Respondant's Sex" * "In general which is more important to you?" Crosstabulation

			"In general which is more important to you?"		
			Convenience	Privacy	Total
"Respondant's Sex"	Male	Count	25	18	43
		% within "In general which is more important to you?"	73.5%	50.0%	61.4%
	Female	Count	9	18	27
		% within "In general which is more important to you?"	26.5%	50.0%	38.6%
Total		Count	34	36	70
		% within "In general which is more important to you?"	100.0%	100.0%	100.0%

In table 4.23 over half of those questioned believe convenience is more important than privacy. Upon closer examination it is clear to see that there is a major difference of opinion between male and female user's general views of privacy. Only 26.5 per cent of female users would rate convenience over privacy but 73.5 per cent of male user's rate convenience as more important. This result was not as expected with slight differences between male and female respondents rather than a 47 per cent difference.

The results for the first sub research objective were a little surprising with not as much of a variation in opinion between male and female participants being expected.

4.3.3 Sub Research Objective Two

The second sub research objective was to examine any differences with students in different areas of study and their awareness of threats to their privacy online. This will be examined in relation to "cookies", "web bugs" and "spyware".

Table 4.39 Awareness level of "cookies" from respondents of different schools

ou ever heard of "cookies" with relation to computing?" * "I am a student of the school of . . ." Crosstab

			"I am a student of the school of . . ."				
			Engineering	Business	Information Technology	Humanities	Total
"Have you ever hearc "cookies" with relatior computing?"	Yes	Count	12	14	16	2	44
		% within "I am a stud of the school of . . ."	54.5%	70.0%	100.0%	20.0%	64.7%
	No	Count	10	6	0	8	24
		% within "I am a stud of the school of . . ."	45.5%	30.0%	.0%	80.0%	35.3%
Total		Count	22	20	16	10	68
		% within "I am a stud of the school of . . ."	100.0%	100.0%	100.0%	100.0%	100.0%

The results of this table were as expected with all students of information technology having heard of "cookies" and only 20 per cent of those studying humanities had heard of "cookies". There was almost a 50-50 spilt with those studying engineering and their awareness of "cookies". Within business 70 per cent of those who participated had heard of "cookies".

Table 4.40 Awareness level of "web bugs" from respondents of different schools

ware of what "web bugs" are in relation to computing?" * "I am a student of the school of . . ." Cross

			"I am a student of the school of . . ."				
			Engineering	Business	Information Technology	Humanities	Total
"Are you aware of wh	Yes	Count	9	12	12	1	34
"web bugs" are in relation to computing		% within "I am a stud of the school of . . ."	42.9%	57.1%	75.0%	9.1%	49.3%
	No	Count	12	9	4	10	35
		% within "I am a stud of the school of . . ."	57.1%	42.9%	25.0%	90.9%	50.7%
Total		Count	21	21	16	11	69
		% within "I am a stud of the school of . . ."	100.0%	100.0%	100.0%	100.0%	100.0%

The results of this table were a little surprising with 25 per cent of those studying information technologies not having heard of "web bugs". Of those studying humanities a large number of those questioned, 90.9 per cent, had not heard of "web bugs" with 90.9 per cent stating they had not heard of "web bubs". In both areas of engineering and business the results were much closer with 57.1 per cent of those studying business and 42.9 per cent of those studying engineering showed awareness that "web bugs" exist.

Table 4.41 Awareness level of "spyware" from respondents of different schools

ı aware of what "spyware" is in terms of computing?" * "I am a student of the school of . . ." Crosstal

			"I am a student of the school of . . ."				
			Engineering	Business	Information Technology	Humanities	Total
"Are you aware of what "spyware" is ı terms of computing	Yes	Count	12	18	14	3	47
		% within "I am a stud of the school of . . ."	57.1%	85.7%	87.5%	27.3%	68.1%
	No	Count	9	3	2	8	22
		% within "I am a stud of the school of . . ."	42.9%	14.3%	12.5%	72.7%	31.9%
Total		Count	21	21	16	11	69
		% within "I am a stud of the school of . . ."	100.0%	100.0%	100.0%	100.0%	100.0%

The results here were as expected with 87.5 per cent of information technology and 85.7 per cent of those studying business were aware of what "spyware" was. Again those studying humanities had the lowest knowledge with 72.7 per cent stating they had never heard of "spyware".

Overall these results were as expected but in some cases there was more of a difference than was expected. The knowledge of business students was not expected to be as high and the information technology student's knowledge was slightly less than expected.

4.3.4 Summary

The overall results for each of the research objectives were almost entirely as expected but with some variations or differences that were not expected. For the main research objective the overall results were as expected with a few expectations. In relation to cookies in table 4.26 the level of security demonstrated was higher than expected with 21.7 per cent of those questioned warned before they accept cookies. Table 4.27 presents some interesting answers in relation to when a user deleted their cookies, this shows results that are not as high as expected. Perhaps the

most worrying results in relation to cookies were shown in table 4.31 with the respondent's awareness levels that cookies can identify user's online habits.

The results of the first sub research objective were as expected but did present a much larger discrepancy between the opinions of male and female respondents than was expected. It was expected to show a slight variation between male and female respondents, but not a 47 per cent difference as shown in table 4.38. This is very worrying, as in the overall results it is shown in table 4.23 there was only 2.8 per cent in the difference between privacy and convenience. In table 4.38 however, it clearly indicated that male users seem to rate convenience much higher that privacy in comparison to female questioned.

The results of the second sub research objective were in the whole as expected with perhaps the most surprising results being the awareness of business students as a whole and information technology student's lack of overall knowledge. Perhaps the most worrying aspect of the results for the third research objective is the lack of knowledge by humanities and engineering students. Even though humanities and engineering students use the Internet on a frequent bases they show a distinct lack of knowledge about threats to their privacy online.

4.4 Conclusion

This chapter provided an overview of the results of the research carried out. Overall the results of the questionnaire were as anticipated, which highlights the lack of knowledge of those students outside information technology. Although information technology students knowledge was not as high as was first expected. This lack of knowledge of possible threats to privacy among these students is worrying as these students also use the Internet to carry out the same tasks as those studying information technologies.

The results of the main and sub research objectives presented outcomes, that although were expected did present the author with some variations that were surprising. The results of the main research objective show cookies as expected as it is presumed "cookies" are the most well known but the knowledge of spyware was higher than had been anticipated. Contained in the results of the first sub research objective was an astonishing variation in opinion of male and female respondents, with females showing much higher awareness than males. The difference in knowledge between students of different schools in the second sub research objective was as expected. However, the knowledge of business students was higher than expected and the information technology student's knowledge was slightly less than expected.

Chapter Five:

Conclusion

5.1 Introduction

This chapter will provide a conclusion of the findings of the literature review and the findings of the study. The chapter will also include the limitations of the study along with recommendations for possible areas of future study.

5.2 Overview of the study

This study examines college student's knowledge of possible threats to their online privacy. The main focus of this study was on the software threats of "cookies", "web bugs" and "spyware". The study began with a review of the literature and the development of the research objectives. The research objectives that were developed were as follows:

Research Objective:

To measure the target population awareness levels of Internet privacy and possible software and tools used by companies to gather their personal information online.

- Which is more important convenience or privacy in term of male and female users
- Are there different levels of awareness of possible threats to online privacy dependent on the student's area of study

Once the research objectives had been developed a research methodology was chosen that would best allow the researcher to answer the research objective. The results of the study were then presented to the reader.

5.3 Conclusion of Literature Review

After the examination of the extant literature it became clear that although there is a large amount of information available on ways in which privacy can be invaded in an online environment there was an apparent lack of Irish studies carried out in this area. The majority of the studies appeared to have been carried out in the US, an example being the Beise et al (2001) study. The literature also provided a very clear and not so pretty picture of the way that companies who gather or have access to personal information treat it. The main focus here is on DoubleClick as they have had very public dealings with privacy groups about their treatment of private information they have gathered. It appears fair to say that there is a lack of definitive and mandatory way for people to ensure their personal information is protected while online as both of the methods discussed are merely voluntary. Therefore, this study was intended to investigate if college students were aware of possible threats to their privacy online.

5.4 Research methodology chosen

In chapter three an examination was carried out on different possible methods that could be used for the study. Once a comparison of the different options available had been carried out it was decided to use quantitative research in conjunction with a questionnaire. A questionnaire with closed ended questions was chosen, as questionnaires can be circulated easily. A quantitative approach was chosen as it is

the most effective in the measurement of awareness levels and the analysis of questionnaires. The target population chosen were students from various backgrounds to show a more balanced group. Students from different age groups were also involved in order to aid a more balanced result.

5.5 Objectives

The main research objective aimed to measure the awareness levels of the target population in relation to Internet privacy and the software and tools used by companies to gather personal information online. The outcome of the study in relation to first research objective was as expected. Cookies were the most well known software among participants to gather information this was expected as cookies are the most common software tool.

Derived from the main research objective a sub objective was developed to measure convenience and privacy factors in terms of male and female users. The outcome of this objective was that female participants rated privacy higher than convenience. This was as expected but such a large disparity in opinion between male and female users was not as expected.

Derived from the main research objective a second sub objective was developed which was to measure the different levels of awareness and different views on online privacy dependent with student's areas of study. The levels of awareness shown by humanities and engineering was lower than was anticipated. However, the knowledge of business students was higher than expected and the lack of knowledge displayed by some of the information technology students was a little startling.

5.6 Conclusion of Study

This study produced results that in general were as expected with a large percentage of those questioned having heard of the most common of the software tools mentioned “cookies”. The level of security that some users had in relation to their cookie policy is reassuring and highlighted that people are aware of some of the possible threats to their online privacy.

The lack of knowledge with relation to “spyware” is the cause of some concern as “spyware” is quiet a common tool. A high percentage of people know what “spyware” is with 68.1 per cent stating this in table 4.35. However, in table 4.36 only 59.6 know the most common way to get “spyware” is by downloading freeware. The most worrying result is people’s unawareness of key loggers in relation to software with only 38.5 per cent of people in table 4.37 stating they were aware of key loggers.

The different views of privacy and convenience between male and female users were not as expected with female users expected to have more of a tendency toward convenience but this was not the case. Studies such as Westin (1998) as cited by Ackerman et al (1999) have shown this to be the case with differences between male and female users and how they view threats to their privacy. It was believed that female users would rate convenience higher due to the usage habits of the Internet, but not the variation that was discovered.

The knowledge of business and engineering students was higher than would have been expected with both sets of students showing a high level of knowledge in the area of tracking devices. The lack of knowledge in some areas displayed by students of information technology was not as anticipated. With 25 per cent of information technology students in table 4.40 stating they had not heard of “web bugs” and 12.5 per cent of information students in table 4.41 not having heard of spyware.

5.7 Limitations

Various limitations were discovered throughout and at the completion of the study.

- Time constraints with the level at which the research was carried out. This study's time frame meant that certain areas prevalent to privacy online could not be examined. The time frame for the study was a period of eleven months but within nine of those months there were other subjects to be considered.

- There were problems with gaining access to enough students to carry out a representative survey. Also the study was carried out at a busy time of year for students due to constraints on the researcher. A further restraint was an inability to gain access to students from certain schools within the college, such as Education and Health Sciences.

- The literature review was restricted where not all relevant research could be accessed and also several of the studies carried out on privacy online were not from reliable academic sources.

5.8 Recommendations for Future Research

Having completed and analysed the research carried out in this field it became apparent that there are areas where future research could and should be carried out

- As pointed out not all schools within Waterford Institute of Technology were included so the expansion of the study to include all schools in the college is a possibility. Also expending the study to other colleges.

- A broader focus would be taken on age, length of time using the Internet and what activities are carried out online as well as which school a student belongs to.

- As a difference was highlighted on the views of male and female students and their views on privacy and convenience further comparison of the views between male and female students could be examined in greater depth.

- Expanding the study for a nationwide study of Irish students and their perception of privacy online and their knowledge on how it can be invaded. This would be a large undertaking but may prove useful in the future.

References

Ackerman, M; Cranor, L.F; & Reagle, J; (1999) “Beyond Concern: Understanding Net Users’ Attitudes About Online Privacy” *AT&T Labs Research Technical Report TR 99.4.3* April 14.

Alster, N; Borrus, A; Green, H; & Yang, C; (2000) “Privacy: Outrage on the Web; A lawsuit against DoubleClick may be just the start of a backlash” *Business Week.* New York: February 14, Issue 3668; page 38.

Baig, E; Gross, N; & Stepanek, M; (1999) “Privacy The Internet wants your personal info. What's in it for you?” *Business Week online* April 5, Issue http://www.businessweek.com/1999/99_14/b3623028.htm.

Baker, W. M; (2006) “WHAT'S YOUR MAIN Technology Concern?” *Strategic Finance Montvale:* December, Volume 88, Issue 6; page 48, 7 pages.

Basile, R. J; Kono, L; & Wong L; (1998) “Web Site Group endorses TRUSTe program to protect privacy of Internet consumers” *Journal of Proprietary Rights.* Clifton: July, Volume 10, Issue 7; page 17, 2 pages.

Beatty, P; Reay, I; Dick, S; & Miller, J; (2007) “P3P Adoption on E-Commerce Web sites: A Survey and Analysis” *IEEE Internet Computing* Volume 11, Issue 2; March-April, pages: 65 – 71.

Beise, C; Perez, J; & Michael E; (2001) “A study of user attitudes toward persistent cookies” *The Journal of Computer Information Systems*. Stillwater: Spring, Volume 41, Issue 3; page 1, 7 pages.

Bennett, C. J; (2001) “Cookies, web bugs, webcams and cue cats: Pattern of surveillance on the World Wide Web” *Ethics and Information Technology Dordrecht:* Volume 3, Issue 3; page 195.

Boyd, H.W; & Westfall, R; (1972) *Marketing Research*, 3rd edition, Richard D. Irwin, Homewood.

Brannick, T; & Roche, W; (1997) *Business Research Methods: Strategies, Techniques and Sources,* Oak Tree Press, Dublin.

Broadhurst, R; (2006) "Developments in the global law enforcement of cyber-crime" *Policing: An International Journal of Police Strategies & Management.* Volume 29, Issue 3.

Broom, R; Forcht, K, A; Gottovi, D; Kruck S, E; & Moghadami, F; (2002) "Protecting personal privacy on the Internet" *Information Management & Computer Security.* Volume 10, Issue 2/3.

Carroll, B; (2002) "Price of privacy: Selling consumer databases in bankruptcy" *Journal of Interactive Marketing* Hoboken: Summer, Volume 16, Issue 3; page 47.

Caudill, M; & Murphy, E; (2000) "Consumer online privacy: Legal and ethical issues." *Journal of Public Policy & Marketing* Volume 19, Issue 1.

Cavoukian, A; & Tapscott, D; (1995) *Who Knows: Safe guarding your Privacy in a Networked World,* Random House, Toronto.

Cooper, D.R; & Schindler, P.S; (1998) *Business Research Methods,* Irwin McGraw Hill, Boston.

Cranor, L. F; (2002) *Web Privacy with P3P* O'Reilly & Associates Inc.

Chung, W; & Paynter, J; (2002) "Privacy issues on the Internet" *System Sciences. HICSS* Proceedings of the 35th Annual Hawaii International Conference on 7-10 January, page(s):9 pages.

Cunningham, P. J; (2002) “Are cookies hazardous to your privacy?” *Information Management Journal* Lemexa: May/June, Volume 36, Issue 3; page 52, 3 pages.

Dasgupta, S; &Turner, C; (2003) "Privacy on the Web: An Examination Of User Concerns, Technology, and Implications for Business Organizations and Individuals." *Information Systems Management* Boston: Winter, Volume 20, Issue 1; page 8.

Davis, J. P; (2007) “Spyware Protection” *Journal of Accountancy* New York: April, Volume 203, Issue 4; page 65, 2 pages.

Downing, D; Covington, M; & Covington M. M; (2000) *Dictionary of Computer and Internet Terms,* 7th edition, Barron’s Educational Services Inc.

Duke, D; (2002) “Spyware, Adware, Systemware and Cookies” *Network Security,* Issue 9, 1 September, Pages 4-5.

Easterby-Smith, M; Thrope, R; & Lowe, A; (1997) *Management Research An Introduction*, Sage Publications London.

Fonseca, F; Pinto, R; & Meira, W, Jr; (2005) “Increasing user's privacy control through flexible Web bug detection” *Web Congress, 2005. LA-WEB 2005 Third Latin American* 31 October - 2 November, 8 pages.

Forte, D; (2005) “Spyware: more than a costly annoyance” *Network Security,* Volume, Issue 12; December, Pages 8-10.

Geer, D; Ranum, M. J; Rubin, A; & Rubin D; (1997) “Web Security Sourcebook: A complete guide to Web Security Threats and Solutions” *America: John Wiley & Sons.*

Goldsborough, R; (2005) “The Benefits, and Fear, of Cookie Technology” *Tech Directions* Ann Arbor: May, Volume 64, Issue 10; page 9, 1 pages.

Graeff, T; & Harmon, S; (2002) "Collecting and using personal data: consumers' awareness and concerns" *Journal of Consumer Marketing* Volume 19, Issue 4; page 302 318.

Gritzalis, S; (2004) “Enhancing Web privacy and anonymity in the digital era” *Information Management & Computer Security* Volume 12 Issue 3.

Hall, S. D; & Larson, L. L; (2000) “Website certification: The TRUSTe alternative” *The CPA Journal*. New York: June, Volume 70, Issue 6; page 72, 2 pages.

Hague, P; (2002) *Market Research; A guide to Planning, Methodology and Evaluation*, 3rd edition, Kogan Page Ltd. London.

Hoinville, G; & Jowell, R; & Associates (1978) *Survey Research Practice*, Heinemann Educational Books, London.

Ibert, J; Baumard, P; Donada, C; & Xuereb, J-M; (2001) ‘Data Collection and Managing the Data Source’, in Thietart, Raymond-Alain, et al. (eds.), *Doing Management Research, a Comprehensive Guide* Sage Publications, London.

Kent, R; (1999) *Marketing Research: Measurement, Method and Application,* International Thompson Business Press, London.

Kierkegaard, S. M; (2005) “How the cookies (almost) crumbled: Privacy & lobbyism” *Computer Law & Security Report* Volume 21; pages 310-322.

Kucera, K; Plaisent, M; Bernard, P; & Maguiraga, L; (2005) “An empirical investigation of the prevalence of spyware in internet shareware and freeware distributions” *Journal of Enterprise Information Management* Bradford: Volume 18, Issue 5/6; page 697, 12 pages.

Luck, D.J; Wales, H.G; & Taylor D.A; (1970) *Marketing Research,* Prentice Hall Inc, London.

McNiff, J; & Whitehead, J; (2002) *Action Research Principles and Practices,* Routledge Flamer, London.

Miller, D.C; (1991) *Handbook of Research Design & Social Measurement,* Sage Publications, C.A.

Milne, G. R; & Rohm, A. J; (2000) "Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives." *Journal of Public Policy & Marketing* Volume 19, Issue 2.

Moser, C; & Kalton, G; (1992) *Survey Methods & Social Investigation,* Heinemann, London.

Moukheiber, Z; (1996) “DoubleClick is watching you” *Forbes* New York: November 4, Volume 158, Issue 11; page 342, 3 pages.

Mujtaba, B. G; (2003) “Ethical Implications of Employee Monitoring: What Leaders Should Consider” *Journal of Applied Management and Entrepreneurship*. Fort Lauderdale: July, Volume 8, Issue 3; page 22, 26.

Nissenbaum, H; (1998) "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy* Volume 17.

Oates, B. J; (2006) *Researching Information Systems and Computing,* Sage, London

Patel, V; & Juric, R; (2001) "Internet users and online privacy: a study assessing whether Internet users' privacy is adequately protected" *Information Technology Interfaces*. Proceedings of the 23rd International Conference on 19-22 June, Volume 1, pages: 193 200.

Patton, M.Q; (2002) *How to use Qualitative Methods in Evaluation,* Sage Publications.

Proctor, T; (2003) *Essentials of Marketing Research*, 3rd edition, Prentice Hall, London.

Saunders, M; Lewis, P; & Thornhill, A; (2007) *Research Methods for Business Students*, 4th edition, Prentice Hall, London.

Shaw, G; (2003) "Spyware & Adware: the Risks facing Businesses" *Network Security,* Issue 9, September, Pages 12-14.

Smith, R. M; (1999) "The Web Bug FAQ" Version 1.0 November 11;
Available http://www.eff.org/Privacy/Marketing/web_bug.html Retrieved April 12th 2007.

Sterling, B; (1993) "Short history of the Internet"
Available http://undergraduate.csse.uwa.edu.au/units/231.312/internet-history.html
Retrieved March 10, 2007.

Stone, M; & Warner, M; (1970) *The Databank Society: Organisations, Computers and Social Freedom,* Allen & Unwin, London.

TRUSTe Available http://www.truste.org Retrieved April 27th 2007.

Vidich, A; & Lymann, S; (1994) 'Qualitative Methods: Their History in Sociology and Anthropology' *in Handbook of Qualitative Research*, Denzin, N; & Lincoln, Y; Sage Publications, London.

Webb, JR; (2002) *Understanding and Designing Marketing Research*, 2nd edition, Thomson Learning, United Kingdom.

Wingfield, N; (2000) "DoubleClick Moves To Appoint Panel For Privacy Issues" *Wall Street Journal (Eastern edition)* New York, N.Y.: May 17, page 1.

World-Wide-Web Consortium (W3C) (2000); "The platform for privacy preferences 1.1 specification", Available http://www.w3c.org/P3P Retrieved April 27th 2007.

Yu, J; & Cooper, H; (1983) "A Quantitative review of research design effects on response rates to questionnaires" *Journal of Marketing Research* 20, 36-44.

Appendix 1

Internet Growth

Internet Growth

Date	**Number of Users**	**% World Population**	**Information Source**
December, 1995	16 millions	0.4%	IDC
December, 1996	36 millions	0.9%	IDC
December, 1997	70 millions	1.7%	IDC
December, 1998	147 millions	3.6%	C.I. Almanac
December, 1999	248 millions	4.1%	Nua Ltd.
March, 2000	304 millions	5.0%	Nua Ltd.
July, 2000	359 millions	5.9%	Nua Ltd.
December, 2000	361 millions	5.8%	Internet World Stats
March, 2001	458 millions	7.6%	Nua Ltd.
June, 2001	479 millions	7.9%	Nua Ltd.
August, 2001	513 millions	8.6%	Nua Ltd.
April, 2002	588 millions	8.6%	Internet World Stats
July, 2002	569 millions	9.1%	Internet World Stats
September, 2002	587 millions	9.4%	Internet World Stats
March, 2003	608 millions	9.7%	Internet World Stats
September, 2003	677 millions	10.6%	Internet World Stats
October, 2003	682 millions	10.7%	Internet World Stats
December, 2003	719 millions	11.1%	Internet World Stats
February, 2004	745 millions	11.5%	Internet World

			Stats
May, 2004	757 millions	11.7&	Internet World Stats
October, 2004	812 millions	12.7%	Internet World Stats
December, 2004	817 millions	12.7%	Internet World Stats
March, 2005	888 millions	13.9%	Internet World Stats
June, 2005	938 millions	14.6%	Internet World Stats
September, 2005	957 millions	14.9%	Internet World Stats
November, 2005	972 millions	15.2%	Internet World Stats
December, 2005	1,018 millions	15.7%	Internet World Stats
March, 2006	1,023 millions	15.7%	Internet World Stats
June, 2006	1,043 millions	16.0%	Internet World Stats
September, 2006	1,086 millions	16.7%	Internet World Stats
December, 2006	1,093 millions	16.6%	Internet World Stats

Source: Internet World Stats: Usage and Population Statistics

Available on http://www.internetworldstats.com/stats.htm

Appendix 2

Internet Usage and Population Statistics in Ireland

Internet Usage and Population Statistics in Ireland

Year	**Users**	**Population**	**% Population**	**Usage Source**
2000	784,000	3,755,300	20.9%	ITU
2002	1,319,608	3,780,600	34.9%	Nielsen NR
2006	2,060,000	4,104,354	50.2%	C.I. Almanac

Source: Internet World Stats: Usage and Population Statistics

Available on http://www.internetworldstats.com/eu/ie.htm

Appendix 3

Questionnaire

Questionnaire

My name is Elaine Colfer and I am a master's student in the School of Science at Waterford Institute of Technology. As part of my master's program I am undertaking a study to estimate people's view of privacy in the online environment.

Instructions

Please only select one option for each question unless otherwise stated.

1. **Are you** male ☐ or female ☐?

2. **Which age group do you fall into?**

☐	17-19	☐	20-22	☐	23-25
☐	26-29	☐	30-35	☐	36-44
☐	45-54	☐	55 or older		

3. **Please select the level of education you have completed**

☐ Primary education or equivalent

☐ Secondary education or equivalent

☐ Third Level education or equivalent

4. **How long have you been using computers?**

☐ Less than 6 months ☐ 6 to 12 months

☐ 1 to 3 years ☐ 4 to 6 years

☐ 7 years or more

5. Do you use the Internet in WIT?

☐ Yes ☐ No

6. What other locations do you use the Internet?

☐ Home ☐ Friend or neighbours house

☐ Internet Cafe ☐ During Travel

☐ Personal Digital Assistant (PDA) wireless

7. How long have you been using the Internet (including using email, gopher, ftp, etc.)?

☐ Less than 6 months ☐ 6 to 12 months

☐ 1 to 3 years ☐ 4 to 6 years

☐ 7 years or more

8. On average how many hours a week do you spend on the Internet

☐ 0 to 1 hours/week ☐ 2 to 4 hours/week

☐ 5 to 6 hours/week ☐ 7 to 9 hours/week

☐ 10 to 20 hours/week ☐ 21 to 40 hours/week

☐ Over 40 hours/week

9. **Have you ever been requested to provide personal information when visiting a web site?**

☐ Yes ☐ No

If no skip to question 12

10. **The reputation of a company is important to you when providing personal information online.**

☐ Strongly Agree ☐ Agree ☐ Disagree ☐ Strongly Disagree

11. **Would you be likely to give your personal information to a web site if you were compensated for it in some way?**

☐ Strongly Agree ☐ Agree ☐ Disagree ☐ Strongly Disagree

12. **Do you use the Internet for personal non-educational use?**

☐ Yes ☐ No

If no skip to question 19

13. **Do you use the Internet to buy goods?**

☐ Yes ☐ No

14. **Do you use the Internet to pay bills?**

☐ Yes ☐ No

15. **Do you use the Internet to listen to the radio?**

☐ Yes ☐ No

16. **Do you use the Internet to download music?**

☐ Yes ☐ No

17. Do you use the Internet to watch movies?

☐ Yes ☐ No

18. Do you use the Internet for general browsing (surfing)?

☐ Yes ☐ No

19. During the last year 2 years have you ordered goods or services over the Internet?

☐ Yes ☐ No

If no skip to question 22

20. If yes, what types of goods or services were ordered?

Please tick all appropriate boxes

Computer software ☐

Computer hardware ☐

Music (e.g., CDs, tapes, MP3) ☐

Books, magazines, on line newspapers ☐

Videos, digital video disc (DVD discs) ☐

Other entertainment products (concert, theatre tickets) ☐

Food ☐

Prescription drugs ☐

Other health, beauty, vitamins ☐

Clothing, jewellery and accessories ☐

Furniture ☐

Electronic goods (e.g., camera, computer, stereo, TV, DVD player) ☐

Automotive (e.g., cars, trucks, recreational vehicles or products) ☐

Travel arrangements (e.g., hotel reservations, travel tickets, rental car) ☐

Flowers - gifts ☐

Sports equipment ☐

Toys and games ☐

Real Estate ☐

Other ☐

21. On average, how often do you make online purchases from Web-based vendors?

☐	Don't buy online	☐	Buy less than once a month
☐	About once a month	☐	Several times each month
☐	About once a week	☐	Several times a week
☐	Other		

22. In general which is more important to you?

☐	Convenience	☐	Privacy

23. Do you consider privacy a major concern when using the Internet?

☐ Strongly Agree ☐ Agree ☐ Disagree

☐ Strongly Disagree

24. Have you every heard of "cookies" with relation to computing?

☐ Yes ☐ No

If no skip to question 31

25. Which of the following "cookies" policies do you primarily use when browsing?

☐ I was always accept cookies

☐ I only accept cookies from the same site I am browsing

☐ I am warned before accepting cookies

☐ I ignore/never accept cookies

☐ I don't know what a cookie is

☐ I don't know what my cookie preferences are set to

26. How often do you delete your "cookies"?

☐	Every time you use the Internet	☐	Once a day
☐	Every second day	☐	Once a week
☐	Every two weeks	☐	Once a month
☐	Once a month or longer	☐	Never

27. Are you aware that "cookies" can track web sites visited?

☐ Yes ☐ No

28. Are you aware that "cookies" can track links on individual web sites visited?

☐ Yes ☐ No

29. Are you aware that "cookies" can monitor whether you are logged in into a web site or not?

☐ Yes ☐ No

30. Are you aware that "cookies" can identify your habits when using the Internet?

☐ Yes ☐ No

31. Are you aware of what "web bugs" are in relation to computing?

☐ Yes ☐ No

If no skip to question 34

32. **Are you aware that "web bugs" are placed on websites to collect information on your online habits?**

☐ Yes ☐ No

33. **Are you aware that "web bugs" gather information on what you are doing online for example what web site's you visit and when?**

☐ Yes ☐ No

34. **Are you aware of what "spyware" is in terms of computing?**

☐ Yes ☐ No

If no thank you for your participant

35. **Are you aware that the most likely way to get "spyware" on your computer is by downloading freeware?**

☐ Yes ☐ No

36. **Did you know that a type of "spyware" called key loggers can track all your username's and passwords while you are online?**

☐ Yes ☐ No

I would like to thank you for your time and co-operation in completing this questionnaire; it will be of great help to me. Best of luck in your future studies.

_____

Elaine Colfer