RISK REDUCTION THROUGH TECHNOLOGICAL CONTROL OF PERSONAL INFORMATION

SHIRLEY ATKINSON

DOCTOR OF PHILOSOPHY

2008

Risk Reduction through Technological Control of Personal Information

by

Shirley Atkinson

A thesis submitted to the University of Plymouth in partial fulfilment for the degree of

Doctor of Philosophy

School of Computing, Communication and Electronics

Faculty of Technology

October 2007

Abstract

Risk Reduction through Technological Control of Personal Information
Shirley Atkinson

Abuse and harm to individuals, through harassment and bullying, coexist with Identity Theft as criminal behaviours supported by the ready availability of personal information. Incorporating privacy protection measures into software design requires a thorough understanding about how an individual's privacy is affected by Internet technologies. This research set out to incorporate such an understanding by examining privacy risks for two groups of individuals, for whom privacy was an important issue, domestic abuse survivors and teenagers. The purpose was to examine the reality of the privacy risks for these two groups.

This research combined a number of approaches underpinned by a selection of foundation theories from four separate domains: software engineering; information systems; social science; and criminal behaviour. Semi-structured interviews, focus groups, workshops and questionnaires gathered information from managers of refuges and outreach workers from Women's Aid; representatives from probation and police domestic violence units; and teenagers.

The findings from these first interactions provided specific examples of risks posed to the two groups. These findings demonstrated that there was a need for a selection of protection mechanisms that promoted awareness of the potential risk among vulnerable individuals. Emerging from these findings were a set of concepts that formed the basis of a novel taxonomy of threat framework designed to assist in risk assessment.
To demonstrate the crossover between understanding the social environment and the use of technology, the taxonomy of threat was incorporated into a novel Vulnerability Assessment Framework, which in turn provided a basis for an extension to standard browser technology. . A proof-of-concept prototype was implemented by creating an Internet Explorer 7.0 browser helper object. The prototype also made use of the Semantic Web protocols of Resource Description Framework and the Web Ontology Language for simple data storage and reasoning. The purpose of this combination was to demonstrate how the environment in which the individual primarily interacted with the Internet could be adapted to provide awareness of the potential risk, and to enable the individual to take steps to reduce that risk. Representatives of the user-groups were consulted for evaluation of the acceptability of the prototype approach. The favourable ratings given by the respondents demonstrated the acceptability of such an approach to monitoring personal information, with the provision that control remained with the individual. The evaluation exercise also demonstrated how the prototype would serve as a useful tool to make individuals aware of the dangers.

The novel contribution of this research contains four facets: it advances understanding of privacy protection for the individual; illustrates an effective combination of methodology frameworks to address the complex issue of privacy; provides a framework for risk assessment through the taxonomy of threat; and demonstrates the novel vulnerability assessment framework through a proof-of-concept prototype.

Contents

List of Figures

List of Tables

Acknowledgements

This research has been made possible by the scholarship awarded to me by the University of Plymouth, for which I am extremely grateful. Profound thanks are also due to my Director of Studies, Dr Chris Johnson who first alerted me to the opportunity. A very deep, and special thanks has to go to my second supervisor, Dr Andy Phippen, who has been an inspiration as well as a source of good discussion and considerate guidance. Thanks are also due to everybody in the Network Research Group for their support.

In conducting this research I was privileged to be allowed insights into the courageous work carried out in the harsh worlds of both domestic abuse and child abuse. I give my heartfelt thanks to those unnamed people who work hard to address the dangers and abuses that the modern world brings. I should like to give special thanks to those members of Women's Aid who work tirelessly for their organisation, thank you for the insights into the dangers faced by Survivors.

I should like thank the young people who took the time to talk to me, your insights have been an inspiration. Thanks too to my own young people, Chris, Colin and Lottie, who all knew not to ask too much of their mother during her studies – of course there was always Bridget!

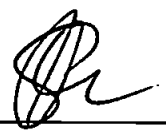
Finally, I should like to give the biggest and most heartfelt thanks to all those men in my life who have demonstrated that there can be supportive, caring and non-patriarchal men in existence. The most notable of these men has to be my husband. Mike, this is for you.

Authors Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award.

This study was financed with the aid of a studentship from the University of Plymouth.

Relevant seminars and conferences were regularly attended at which work was often presented and several papers prepared for publication. These are attached in the appendices.

Signed 

Date 22/1/08

1 Introduction

This chapter introduces the context of this research, by providing a brief summary of the main issues surrounding personal privacy. The resulting potential for harm arising from interactions with Internet technologies is introduced. The aims and objectives of this research are presented, and the chapter concludes with a summary of the thesis structure.

1.1 Personal privacy and the potential for harm

The intersection between Internet technologies and personal data creates a potential for harm that is of increasing concern. Technology has become an integral element within everyday life, and so the effect is felt by an individual irrespective of whether they make explicit use of technology or suffer the consequences of third party actions. Increasingly technologies are linked together through Internet protocols, and so information about the individual in terms of location, name, address, date of birth, preferences and dislikes, are all easily transmitted around the globe. New devices are increasingly Internet-enabled to share in this web of transmission in the name of increasing efficiency. For example, the location of a mobile phone allows for tailored travel information to be accessed through the Internet allowing for quicker and more relevant information retrieval.

Conflicting and outdated legal approaches cause dilemmas and issues in this fast moving field and legal redress is subject to an imbalance of power, when only those with access to funds can seek legal redress and protection from the abuse of information. In the commercial world, the collection and manipulation of large amounts of personal information underpins their activity, making the data about the individual very attractive to the business enterprise. This lends itself to a tension between providing convenience for

the individual, and yet engendering a trusting environment. Increasingly, the political influence is felt with public data becoming widely and easily available, yet the education campaigns backed by the government seek to inform individuals about the dangers of giving out their personal information.

From the technological side, the Internet is becoming a much more social space. Information is easier to share between friends, but as yet unknown friends can see information about the individual's everyday life too. The Semantic Web aims to improve the interoperability of data by formatting it into predefined and widely accepted standards, thus allowing machines to infer and reason with it. Mobile technologies are converging in such a way that facilitates the interaction with the Internet irrespective of location. Add to these elements the increase in easily available surveillance technologies, and the move towards the aggregation of disparate pieces of information, and there arises a potential for harm.

The issue is not, in itself, the release of personal information, but the fear of and use of information for abusive or damaging purposes. Privacy Enhancing Technologies [PET's] have their limitations, they require explicit protection choices to be made, and they do not address the issues that certain members of society face. Some individuals are more at risk from invasions of privacy and the abuse of personal information than others.

Addressing the potential for harm represents an important area for research, allowing an understanding of risks to be integrated into software design, to bring about a risk management approach accessible to the individual. The focus for this research has been

upon the individual and how technology can assist in self-protection.

1.2 Aims and objectives

The aim of this research has been to define, design and validate a potential software architecture that can assist the individual in risk reduction through controlling their personal information. This has been achieved by exploring the risks encountered by selected groups of individuals and incorporating that understanding into the architecture.

In order to achieve this aim, the following objectives were defined:

1. To gain a clear understanding of risks and the distribution of risks;
2. To develop a taxonomy framework to assist in the identification of risks;
3. To develop a design for software that allows for technological control of personal information, adaptable to the context of the individual;
4. To implement a prototype of the design;
5. For user-groups to evaluate the prototype in order to gain an understanding of the acceptability of such a software solution.

The first objective provides a clear understanding of how the risks of harm manifest for some individuals. Based on this understanding, a comprehensive argument is made for the need for a risk management approach.

The second objective incorporated the understanding of risks into a taxonomy framework to enable future risk assessments to be carried out. Following the application of this

taxonomy to two separate areas for validation, the third objective sought to incorporate the taxonomy framework into a software design. A design architecture for software incorporating some elements of the Semantic Web was created and the fourth objective set out to implement a proof-of-concept of the design.

The fifth and final objective required a return to the selected user-groups for an evaluation of the acceptability of such a software approach.

1.3 Structure of thesis

Chapters 2 and 3 situate this research through exploring the complex background to personal privacy and introducing the potential for harm. This is achieved by chapter 2 exploring the myriad of influences on personal privacy, brought about by the intersection between personal data and Internet connectivity. Consideration is given to the relevant legal, commercial, political and social influences.

Chapter 3 follows on by exploring the potential for harm by conducting an examination of the harm categories of financial loss, altered behaviour and mental or physical harm. These are followed by a critique of the current solutions and the chapter concludes with an overview of the Semantic Web.

Having firmly established the need to investigate in more detail the potential for harm, chapter 4 considers the methodology forming the foundation for this research. Here the chosen epistemological approach is discussed, along with the relevant foundation theories. This research design is considered and the chapter concludes with a reflection

on the methods.

Chapter 5 introduces the first objective by presenting a plan of the implementation of the research methods outlined in chapter 4. The findings from the study of the selected populations are described and discussed, and the emergent framework categorising encountered risk areas is presented.

Chapter 6 presents the second objective by establishing the use of taxonomies within risk assessment, starting with a consideration of the limitations of existing taxonomies. This chapter presents a novel taxonomy of threat built upon the knowledge gained of the categories of risk in chapter 5. The individual components of the taxonomy are described and validation carried out by applying the taxonomy in two separate areas of social networking and mobile phone usage within an educational context.

Chapter 7 introduces the third objective by discussing the requirements and functionality required of a software design. A Vulnerability Assessment Framework (VAF) is introduced to implement concepts from the taxonomy of threat. The chapter concludes with an introduction to the Semantic Web in conjunction with an outline of a proposed architecture to implement the VAF and incorporate elements of the Semantic Web.

The fourth objective is presented in chapter 8. This chapter describes the implementation of a proof-of-concept prototype of the software design. The three key pieces of functionality that were implemented are described. These were to:

1. Manage privacy settings;
2. Receive threat notifications; and
3. Manage personal information divulged to websites.

The fifth and final objective is presented in chapter 9. The approach taken for evaluation is described, along with the interactions with the user-groups. The findings from the evaluations are presented and the chapter concludes with a discussion surrounding the implications for the implementation of the prototype.

Chapter 10 presents the main conclusions to be drawn from this research programme, highlighting the key achievements and discussing the limitations. Considerations are outlined for further research and the chapter concludes with a personal view of the field of personal privacy. This thesis provides a number of appendices in support of the main discussion, including questionnaires and code listings. These appendices also contain a number of published papers arising from this research programme. The majority of papers were written with guidance and support from the supervisory team. One paper however, by Wood et al [2007], was the result of an equal collaboration with a researcher involved in teacher training.

2 Personal Privacy

This chapter begins by providing the background for this research by examining the literature surrounding personal privacy. The major influencing factors are introduced and discussed.

2.1 Background

Privacy has progressed from the original concepts of natural privacy, where moats and drawbridges provided a barrier to unwanted intrusion, to more modern concepts that include the control of personal information. This differentiation is expressed by Moor [2000], who drew a distinction between *natural* privacy, where physical boundaries served to protect individuals, and *normative* privacy, which describes a socially determined need for protection.

Stalder [2002] considered privacy in terms of a boundary separating the individual from their environment. One side of that boundary was public and the other private. Quinn [2005] extended the boundary argument to include the issues surrounding accessibility to an individual. These accessibility issues occur when balancing the desires of those who want access to an individual, against the individual's desire to remain separate.

The modern definition of privacy has moved away from physical concepts to encompass the notion of control of information about the self. Discussion on privacy now explicitly considers the exercising of control over the flow of personal data between entities [Westin, 2003; Schwartz, 1999]. The right of individuals to control their personal information is included [Garfinkel, 2000] as is the freedom of choice over confidentiality of elements of

personal information [Cavoukian and Tapscott, 1997]. Cannon [2004] emphasises the need for developers to ensure compliance with personal wishes about privacy when developing applications that handle personal data.

Privacy has been described as multi-dimensional: Clarke [1999] proposed that there were four dimensions to privacy:

- personal – physically taking samples from the individual, DNA for example;
- personal behaviour – choice of religion, or political allegiance;
- communications – ability to communicate without being observed; and
- data or information privacy.

Tavani [2007] however, categorised the dimensions in a different manner making three dimensions:

- accessibility privacy – the physical freedom from intrusion;
- decisional privacy – freedom from interference in choices and decisions; and
- informational privacy – the control over the flow of personal information;

Privacy has been identified as being highly subjective [Raab, 2004]. Certainly Hine and Eve [1998] discuss how individuals perceive privacy invasion based upon context. At the time of writing those in receipt of child benefit are likely to have privacy concerns. Parents have received letters from the HM Revenue and Customs apologising for the loss of CDs containing their personal details which include the bank or building society into which their

child benefit has been paid. The potential for identity fraud has been highlighted by the media [BBC, 2007]. The complexity of the circumstances that can combine to create the privacy invasive situation were highlighted. This complex mixture of elements included the:

> "*visibility of a mediating technology; the perceived legitimacy of information requests ; the representation of intrusion or disruption of legitimate activity; perceived imbalances of power and control; and representations of the social context.*" [Hine and Eve, 1998]

Personal privacy, in the context of this research, is a construct created from the complex interaction of many differing factors. These factors range from external influences upon an individual to more internalised behavioural issues. Legal controls provide elements of protection for personal data and constraints for commerce; personal data is collected and manipulated by commercial activity; government policy dictates the collection, maintenance and distribution of publicly available personal information and influences education campaigns which seek to highlight concerns and influence behaviour; individuals maintain their social connections; and throughout these elements, technology provides a steadfast theme. The next section of this chapter discusses each of these external influences in more detail.

2.2 Legal Influences

The global nature of the Internet brings complexities in terms of jurisdiction. An individual interacting with a website that collects and stores personal information can involve a number of countries and their individual privacy laws. General Motors found this to their cost when attempting to create an online telephone directory [Windley, 2005] – they spent two years negotiating the different privacy laws covered in their multinational dealings.

Should an individual wish to seek redress for harm done, they first need to ascertain exactly where the infringement of privacy took place, where the defendant is located and which law is relevant. This myriad of pieces of legislation makes it almost impossible to provide a uniform privacy approach; one legal approach that suits one country may be intolerable within another. No doubt this international dimension affects the privacy of individuals, but because the participants for this research were all based within the United Kingdom (UK), the focus is therefore upon those laws that have the most effect upon UK citizens.

Richards and Solove [2007] propose that UK and US laws have diverged as a result of a landmark case in the late 1800s. The Prince Albert vs Strange case was the primary influence for the paper by Warren and Brandeis [1890] where privacy was defined as being the "right to be left alone". Legal protection was proposed for individuals affected by the combination of technologies of the time, cheaper photography, as provided by the inexpensive cameras created by the Eastman Kodak company, in combination with the emerging tabloid media which had seen readership increase substantially. Prominent individuals began to have photographs and stories about themselves published in tabloid newspapers and thus turned to the law for redress. Since then, US law has concentrated on protecting individual's against invasions of privacy by others. Protection has been based upon intellectual property rights and maintains that, whilst people are free to give out their information to whom they choose, they assume any risk of betrayal by doing so. Information given out is no longer deemed to be private, creating a binary relationship between what is public and what is private. This binary approach is not echoed within the UK law which is based on confidentiality. Confidentiality within the UK law is in turn based

upon social expectations of non-disclosure and recognises that there are intermediate stages between public and private information [Richards and Solove, 2007].

There is also a conflict in approach between the US and the European Union (EU), especially surrounding the collection and onward dissemination of personal data [George, 2004]. The US privacy laws are very much based upon upholding rights, whereas the EU laws take a data protection approach, an approach which Bartow [2000], in a comparison between the EU Data Protection Directive and the US Children's Online Privacy Protection Act (COPPA) 1998, argues gives European adults more privacy protection than US children. The manifestation of the US approach is heavily biased towards self-regulation and conformity to policy, with the privacy policy as a central tenet. In an attempt to balance the tensions between the two approaches, the US Department of Commerce and the European Commission drafted the Safe Harbour Agreement. This agreement sets out the restrictions required on the collection and onward dissemination of personal data. American companies that wish to trade with European countries self-certify that they have comprehensive procedures and policies for data protection in place [Russell, 2005]. UK citizens are very likely to encounter the differing UK, EU and US models for privacy protection during their interactions with the Internet. Privacy laws are most usually articulated through either the privacy policies or the terms and conditions of websites, and only **if individuals choose to read these policies** will they be aware of which legal privacy paradigm is prominent. One example is with MySpace, which even though the individual may be signing up within the UK, the privacy policy states that the individual is agreeing to be bound by the US laws on privacy protection.

The EU law seeks to maintain a balance between those that would utilise privacy to conceal wrongdoing and protection of the individual. Articles 8 and 10 of the Convention of Human Rights [Council of Europe, 1950] enshrine the right to privacy of the individual and set out the principles for freedom of speech. Article 10 provides the state with the right to intervene should it perceive a threat to the "economic well-being" of the country, or to limit the freedom of an individual in order to protect others. The European Court of Human Rights is where cases against those state interventions are heard [Colvin, 2002].

Schoeman [1984] argues that the law is the only way to protect privacy within developed society, but that there are shortcomings in that individuals do not necessarily have the required skills or information in order to exert control over their personal information. The law requires active participation, whereby individuals explicitly exercise their right to privacy through remedial court action [Solove, 2003], thus building case law and precedent. Legal redress concentrates on rectifying harm done to the individual, but does not account for any social or cultural factors [Raab, 2004], for example individuals may not feel empowered enough to take legal action either because of social status or financial status, or may be distrustful of those involved in the legal system.

To keep up to date the law requires active, regular oversight and enforcement to be effective. Privacy, however, has a broad scope and changes rapidly with the influence of technology [Gellman, 1997] therefore keeping up to date becomes difficult. Cases within the last four years have involved digital rights management, protection of copyright and intellectual property rights (IPR). These cases appear to be the subordination of one set of rights over another [Leenes and Koops, 2005], illustrating an imbalance of power where

companies have the financial wherewithal to resort to law and can exert their rights over the rights of individuals. Difficulties also arise where judiciary and members of the jury may perhaps have little engagement, or knowledge of technology or it's use. This can lead to situations where they pass judgements that create precedents leading to a detrimental approach to privacy. At the time of writing a judge has been criticised for asking the question "what is a website?" [Page, 2007], inviting an assumption to be made whereby the judiciary have little knowledge of what might appear to some to be everyday technology.

The success by corporations in utilising IPR has prompted Bartow [2000] to suggest that individuals could benefit from this approach. If personal information was considered in terms of IPR for an individual, protection for that information could be afforded through the IPR mechanisms that work so well for companies, thus allowing the same benefits to be felt by companies and individuals alike.

2.3 Commercial Influences

Commercial activity is about trade: businesses trade goods or services with an objective of making a profit from that activity. Successful achievement of the profit objective relies upon the business being competitive and efficient. Technology and it's interaction with personal data, plays an increasingly important role within the commercial enterprise, even for those that do not have a technology focus to their goods or services. Interaction with individuals, both the staff within the business and those the business serves, has altered under the influence of a number of technological changes. For example credit and background checks are utilised for customers and staff members; marketing increasingly

relies on gathering personal information as an important part of any customer relationship strategy and has a knock-on effect on consumer attitudes and trust. Business processes involved in the supply chain or provision of goods and services have become more efficient through the use of technology. Item level Radio Frequency Identifiers (RFID) have the potential to affect personal privacy. Finally, there are an increasing number of commercial opportunities opened up by the convergence of digital media, such as mobile phones and location based services.

2.3.1 Credit and background checks

Staff members are a very important element of any commercial enterprise and finding the right members of staff requires making use of all the techniques open to the recruiters. Recruitment websites allow people looking for work to register themselves as interested in specific positions, to post their job profiles online and, increasingly, candidates are subject to a wealth of background checks. Those working in any position involving contact with young people and vulnerable adults are routinely checked through the Criminal Records Bureau (CRB). These checks are carried out for both volunteers and paid staff. Background checks can now be run on individuals looking at gaps in employment history, checking qualifications and checking the Internet for any public information about that individual. Within the financial sector, those with poor credit history are deemed to be too much of a risk to employ [Carins, 2005; Backgroundchecking 2007]. Social networking websites are increasingly coming under scrutiny for providing information about candidates [Finder, 2006], and even those where the profiles have been made private, or friends only, have been accessed by employers who have requested information using specific legal means [Gray, 2007].

2.3.2 Consumer Profiling

Consumer information forms an important component of Customer Relations Management (CRM). This is an approach designed to various areas of the business enterprise from support sales and marketing, contact centre management and business intelligence [Kobielus, 2007]. The ethos is to understand customer needs as a way of engaging with those customers in a more profitable fashion [Vence, 2007]. Lager [2007] suggests that all companies, irrespective of size, should manage customer information even if it is just account history and communications. The argument here is that customers are far more demanding and aware, and therefore an improved relationship, from the company perspective, can be built with the customer through understanding their habits and preferences.

Understanding the consumer's habits and preferences involves collecting large amounts of information about them. This consumer profile information is used for targeted marketing, whereby large amounts of personal data is data mined by recommender systems to generate consumer purchasing patterns and predictions of future purchasing behaviour [Tavani, 2007]. Chellappa and Gin [2005] describe how personalisation tailors both goods and shopping experience to the individual, using technology for information acquisition and processing to build a profile about personal preferences. Examples of recommender marketing is quite clearly seen with websites such as Amazon, Gmail, and iVillage. Amazon make extensive use of previous purchasing history of the individual. When an individual logs in to their account, they are presented with recommendations of books, CDs and other related goods linked, however seemingly tenuously, to previously purchased items. For those who make frequent use of Amazon, a large profile of the

individual can be discerned with their preferences for music, reading matter and perhaps religious or political viewpoints. Gmail is the Google email service, where emails can be categorised for easier retrieval at a later date. All emails are scanned and advertisements that are relevant to their content are shown alongside them [BBC, 2004]. Google maintain that this process is entirely automated so that humans do not view the content of the email, and neither the content of the emails nor personal details are passed on to the advertisers [Google, 2007]. The iVillage site states:

> *"iVillage.co.uk offers women a 24 hour resource in which to find and share advice. Join like minded women to exchange views, advice, information and support on subjects such as parenting, careers, computers, diet, fitness, food, relationships and working from home."*

However, within this website the pages that offer advice have targeted advertisements showing recommended products. This brings into question how impartial the advice is likely to be [Bartow, 2000].

Personal data has proved to be both an asset and to provide a new commercial opportunity. In bankruptcy cases, databases of customer details have been sold [Tynan, 2005; Tavani, 2007]; the big supermarket chain Tesco owns the Crucible, a subsidiary database that collects detailed information on every household in the UK, and sells access to this information [Tomlinson and Evans, 2005]. Companies such as Paoga (www.paoga.com) and M-Tech Information Technologies Inc (www.mtechit.com) provide identity management or data management services, the latter being aimed primarily at the individual, the former being more for the commercial enterprise.

Building consumer profiles occurs both online and offline. The "loyalty" schemes in supermarkets store all transactions in large databases and create targeted promotional offers by analysing details of purchasing habits and preferences. Tesco, for example, have been collecting purchasing data for many years following the introduction of their loyalty card scheme and many of the other supermarkets have followed suit. Collecting personal information is even easier online, as the data can automatically be stored into databases ready for analysis and further use. Collection can be carried out in both an explicit and implicit fashion. Purchasing goods or services requires the explicit collection of personal information for delivery or to verify credit card payment. Games, fantasy worlds and competitions collect personal information for later use [Valongo, 2000].

Clickstream data is part of the implicit collection of data containing:

- information about the Internet Service Provider (ISP);
- hardware platform;
- software; and
- linking website.

Information about browsing habits and attention spans are gleaned by analysing this information which in turn feeds into either website design or marketing. At the time of writing, there has been discussion on some websites about ISPs selling on clickstream data and the potential this has to identify individuals [Blodget, 2007; Slashdot, 2007; Techdirt, 2007]. These concerns are not new, having been raised in June 2006 in the

Washington Post [Goo, 2006] when comment was made about the AT&T privacy policy that stated clickstream information on AT&T branded websites was to be sold. Hitwise [2007], a company specialising in providing information about consumer activity, advertise on their website that they collect anonymous information from many ISPs within different international markets. Determining the reality of the practice and how widespread it is has proved difficult for Wired [2007], who have received very few responses to their specific questions to Internet Service Providers regarding clickstream retention and dissemination.

Culnan and Bies [2003] propose that the covert collection of information would lead to a tension between the individual and the commercial enterprise, suggesting that many consumers would find methods of collection and use of personal information unfair. Whilst there is a question over whether many individuals realise they are being tracked, consumer attitudes towards the collection of personal information are changing. Cranor and Garfinkel [2005] and Samarajiva [1997] have argued that once consumers begin to distrust a business, false or misleading information will be given, or, in other cases, lack of confidence in how data is treated may lead to lack of engagement with e-commerce [Basbas, 2006]. In this vein, Windley [2005] suggests that consumers will willingly part with their information if they perceive that the company is giving good value in return. Commercial enterprises therefore have to account for both the security concerns of their customers and to abide by the rules and regulations that the relevant legal or industry framework dictate. Privacy policies and seals of approval from third parties such as BBBOnLine, CPA Web Trust and TRUSTe are seen by some as building blocks towards engendering trust with the consumers [Grindin, 2000].

2.3.3 Business Processes

Success for the commercial enterprise requires business processes to be as efficient as possible, and technology is considered as the tool to streamline and expedite those processes. However, this approach is not without controversy, and the examination of why technology fails to deliver proposed benefits, is a large research area in its own right. The distance between the suggested benefits of a technology and the reality, is illustrated by the Gartner hype-cycle [Gartner Group, 2005] between the "Peak of inflated expectations" and the "Trough of disillusionment, illustrated in Figure 1 below.

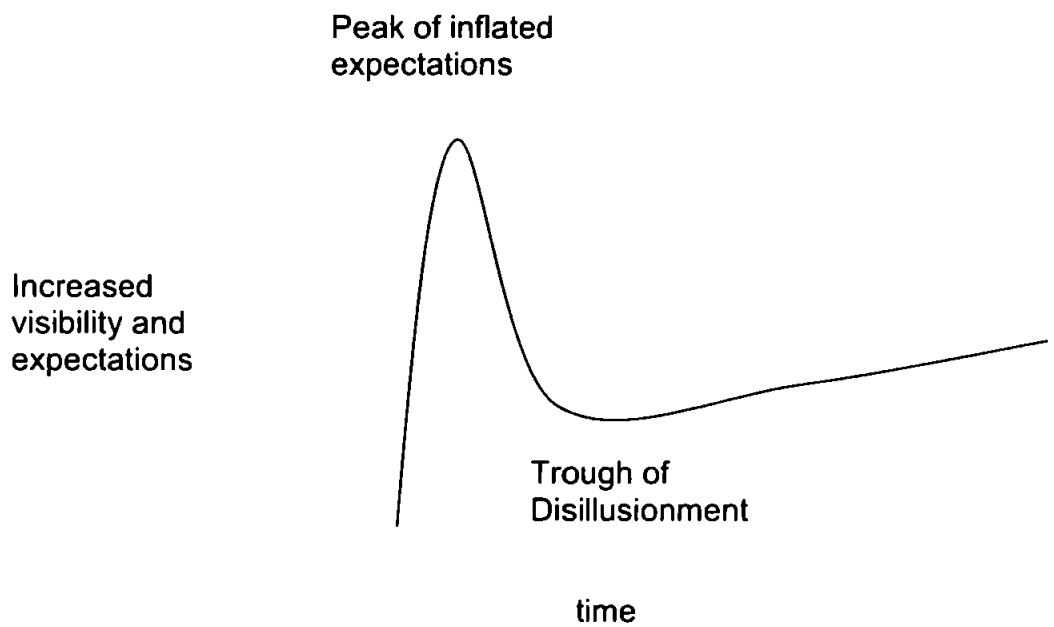


Figure 1: Hype cycle of new technologies. [Source: Gartner Group, 2005]

Baskerville and Land [2004] discuss how technology has a seriously detrimental effect on organisations, especially when information systems inhibit or impede social interactions necessary for business processes to be effective. They describe information systems as being either inwardly or outwardly destructive, either leading to unstable and unsustainable business processes, or where there is damage to the organisation itself.

Because personal information about the individual is manipulated within many business processes, the control, access and management of that information has become an important socio-cultural element. At the time of writing, the management of personal information by government bodies has been criticised by the Information Commissioner, Richard Thomas [Mulholland, 2007]. It remains to be seen whether this becomes what Bakserville and Land [2004] would consider as a destructive facilitator.

Examples of where personal information forms an important element of a business process can be seen in the financial sector. Valuations for mortgages can be carried out from the company desktop. For those situations where the ratio between mortgage and property value falls within certain boundaries, valuations can be carried out making use of combined databases [Rightmove.co.uk, 2007]. Personal information is required when financial institutions contact their customers, the individual who answers the telephone call must validate themselves against the information held by the company. From personal experience, members of the household have been contacted by telephone during an evening or weekend. The operator, before explaining exactly who they are, which company they are from or what the telephone call is to be concerned with, have requested in rapid succession many elements of personal data for their security checks. The requirement being that, prior to embarking on any form of conversation, the person on the receiving end of the telephone call has to verify themselves. However, this creates a situation of imbalance, because the receiver of the telephone call has no method of validating who has made the call.

Supply chains, networks where goods and objects are coordinated between different

organisations and bodies, require that these goods and objects are accounted for properly. Radio Frequency Identifiers (RFID) are utilised providing beneficial approaches to keeping track of items, useful for inventory and control [Collins, 2005]. RFID chips are small electronic chips that contain identifiers and use radio signals to communicate. These chips emit a signal containing a unique ID code when a signal from a reader is received. The received radio signal delivers the power required for the chip to emit a response [Granneman, 2003]. There has been mixed success with the introduction of chips for item level tagging. Comet, Iceland and Woolworths have run RFID trials but abandoned them [Roberts, 2005]; Tesco suffered bad publicity when running a trial with tagged razor blades that recorded customers selecting the blades from the shelf without warning the customers they were being monitored. Tesco have now introduced the chips for tracking palettes of goods [Oates, 2004]; Marks and Spencer now use these chips on many of their clothing items with the labels clearly marked as "Intelligent Labels". The privacy concerns surrounding the use of RFID chips concentrated on the items being linked to the individual, through a combination of tag information, credit card or shopping profiling database [Garfinkel and Rosenberg, 2006].

2.3.4 Convergence

As digital media converge, new opportunities arise that, in turn, may affect personal privacy. One such example concerns itself with the location of an individual as determined through their mobile device. Mobile network operators allow third parties to access the functionality that pinpoints the location of a mobile handset. Additional services are created that provide tailored content according to the location of a given mobile phone. These services range from having location relevant content delivered to the individual

through their mobile phone, to the physical location of the mobile phone being divulged to another party, who will visualise this information by using Internet mapping software. Location based services such as ChildLocate, Sprint Family Locator, traceamobile.co.uk and followus.co.uk offer services to parents who wish to know where their children are. Other markets targeted are delivery drivers and employees and with the use of Global Positioning Systems (GPS) the tracking service is no longer tied to the mobile phone [Technology Quarterly, 2006]. Trafficmaster have incorporated automatic number plate recognition into their traffic cameras that cover the majority of Britain's roads, and sell the information calculated about traffic flow. These blue cameras are seen on many bridges crossing the motorways and main arterial roads and are linked together to provide the three main services of satellite navigation, vehicle tracking and traffic flow information [Trafficmaster, 2007].

2.4 Political Influences

Within the UK, the political influences on privacy arise from mandatory personal data collection by government departments for public sector services. Some of this information has always been available to the general public, for example the electoral roll or civil registration details. Most data collected are accessible only to specified individuals or public and private sector organisations who have valid reasons for access, perhaps because of the services they offer. In 2000 the Cabinet Office proposed that all local councils services should be delivered online by December 2005 [Cabinet Office, 2000]. The effect of moving these local council services online is that those wishing to access public information collected on individuals no longer need to visit the government departments for themselves. Visiting the relevant website saves time because each

relevant department or area is available in one place. At the time of writing, access to large quantities of public information has been facilitated through the use of the Internet.

Within the UK, under certain circumstances, there is mandatory collection of personal data and individuals have no choice but to provide that personal information. In some instances, this mandatory, public data is made freely available. These public records are found in the main areas of:

- Land Registry;
- Civil Registration;
- Planning applications; and
- Company Information.

Not all public sector agencies make the information freely available to members of the general public, some have a more restricted approach to access to data collected. These are:

- the Driver and Vehicle Licensing Authority (DVLA);
- Identity and Passport Agency;
- Police records; and
- the National Health Service.

Policy interventions that surround data sharing, surveillance and funding opportunities for technologies used in surveillance also have an effect on individual privacy. These are all

explored in more detail below.

2.4.1 Public Records

The Land Registry was established in 1862 and has responsibility for maintaining the register of land titles and recording any dealings with those titles, for example mortgages and re-mortgages [Land Registry, 2007]. Searching for information from the land register is now available to the general public through the Land Registry website and for a nominal fee of £3.00 the plan or register of any property can be downloaded. The Land Registry supplies information about the final value of a property to third party websites such as www.ourproperty.co.uk or www.upmystreet.com.

Civil Registration started in 1837 when all births, marriages and deaths were required to be recorded at a local Register Office, the details of which are compiled into a national register. Registrations that have occurred since 1984 are kept in a searchable database. Registrations prior to that are shown as image files of the register. Local registers have always been available to visitors to Registry Office and the national registers have been available previously at St Catherines House in London and in more recent times at the Family Record Centre in Islington. Access to the national registers are now available online both from the General Record Office and through third party websites. Third party websites that charge for access have recently emerged fuelled by the recent interest generated by television programs showing how to research family history. Websites such as www.findmypast.com and www.ancestry.co.uk provide access to lists for a fee, however one large body of volunteers is transcribing the national registers, census data and parish registers for free and making them available at www.freebmd.org.uk. The

national registers offer the basic information that enables a copy of the certificates to be requested through the General Record Office website [GRO, 2007], such as the year; quarter if prior to 1984, month post 1984; the volume; and index entry.

The National Planning Application Register provides online access to all planning applications made across England and Wales for the last twelve months. Local authorities offer access to their own planning applications giving details of the plans, the applicants and the agents. In some councils all documentation is scanned and copies made available online.

Companies House maintains the UK Government register of UK companies and provides an online service to check the status of all registered companies. Directors of all registered companies are required to provide their home addresses and this information is made available to the public. The website 192.com provides a search service that accesses directors reports from companies house and combines it with electoral roll records, both historical and new, along with any telephone directory information held by British Telecom.

2.4.2 Restricted Access

The Driver and Vehicle Licence Authority at www.dvla.gov.uk/ maintains the register of all drivers and vehicles and has responsibility for the collection of Road Fund duty. Interaction for motorists has moved online with the recent introduction of the Vehicle and Operator Services Agency (VOSA) central database for MOTs. MOT certificates are required for all cars over three years old to be deemed roadworthy. Tax discs for vehicles

can be purchased online provided that the car has a new style MOT, that is it has an entry in the MOT database, and the driver and vehicle are registered on the DVLA database. These link up with the Motor Insurer Database to verify that the driver holds valid current insurance for the vehicle and a tax disc can be purchased online [DVLA, 2007]. Driver details are sold by the DVLA to registered companies such as car clamping firms and those who run and maintain car parks [Oates, 2006].

Obtaining passports is changing with the renaming of the UK Passport Agency to the Identity and Passport Service, combining the issue of passports and identity cards into one agency. UK Passports now contain RFID chips that carry a copy of the printed personal information so that checks can detect any tampering with the passport. The Home Office Website [Home Office, 2007] gives a very brief mention of the chip incorporated into the passport, and declares that it can only be read by an e-passport reader. The National Identity Register containing details of every individual within the country is proposed to be created from three existing databases, the Department of Work and Pensions Customer Information Service, the Identity and Passport Service and the Immigration and Nationality Directorate [BBC, 2006a].

The collection of data within the public sector is increasing with proposals for fighting crime. DNA is now routinely taken as part of police enquiries for the National DNA database [Davies, 2000] and surveillance of public spaces through CCTV is commonplace [Garfinkel, 2000]. Connor [2005] reports on the national database for vehicle movements that is stored alongside the Police National Computer at Hendon, which since the beginning of 2006, has been recording the time, date and location of vehicles using

automatic number plate recognition facilities. Chief constables are hoping to link this database with petrol forecourts and garages so that stolen vehicles can be identified quickly [Tendler, 2005].

Medical details are undergoing radical transformation with one of the biggest government IT programs currently taking place. The aim is to provide access to all medical records through NHS net to those medical professionals who need access [NPFIT, 2005], which includes not only front line medical staff, but access for secondary uses such as research. One example is the National Cancer Registry where details about treatment and survival rates are aggregated and analysed to provide data for research [Department of Health, 2007]. Following on from the implementation of the National Strategic Tracing Service (NSTS) where the demographic details of all the NHS patients in the UK were stored, the government has now created the Integrated Care Record Service. This is a complex structure comprising a data spine which will be accessed by different areas around the country. Within the system individuals are identified by their NHS number, a unique 10 digit number issued to them at birth or on entry to the NHS system. A central issue system allocates the NHS number which is then to be used on all hospital correspondence, allowing all relevant interactions to be linked to the one patient [CFH, 2007].

2.4.3 Data Sharing Policy

The DfES are beginning to create the Children's information sharing index, now called Contact Point [DfES, 2007]. This will collect full personal data about the child, their name, gender, date of birth, parental details, school details and achievement details [ARCH, 2007]. Currently, London authorities have been involved in piloting the index and selected

authorities will roll it out during 2008.

With the policy agenda entitled "Transformational Government" individuals can expect to see more of their personal data collected and shared between the public sector agencies [CIOC, 2007]. Whilst there is more to this government policy than is described here, only that relevant to the focus for this research is discussed. The purpose of this strategy is to ensure that public services can be delivered more efficiently through the use of technology. Services are to be shared where possible, so end the duplication of services, and situations, where the same information has to be given to many government departments. The two main aims of the policy, the delivery of public services and the sharing of information between public services and systems has the most effect on the privacy of individuals. Sharing information has made life easier for some, for example, the ability to purchase car tax online as discussed earlier in section 2.4.2. Future combining of services include: the ability for the Department of Work and Pensions (DWP) to automatically gather information to calculate entitlement to Council Tax for those claiming pension credits; to allow information sharing under the Social Exclusion Action Plan, primarily where services are delivered to adults who "*lead chaotic lives and have multiple needs*"; provide quicker information to relevant services about recently deceased individuals so that identity fraud can be prevented [HMG, 2006]. Underpinning this delivery of shared information and services is the requirement that all individuals can be clearly and uniquely identified [Suffolk, 2006].

Home Office influence upon surveillance technologies that record and monitor individuals is seen clearly in its investment in CCTV, research into better recognition technologies and

interest in the use of biometrics. The report from the Royal Academy of Engineering [2007] released in March this year observed that the government expenditure on CCTV for the UK Government has risen dramatically. The irony has been pointed out whereby George Orwell's flat in central London has been observed as being monitored by 32 CCTV cameras [Evening Standard, 2007]. Orwell was the author of the book 1984 where ordinary individuals were monitored by "*Big Brother*". The Home Office Scientific Development Branch HOSDB, [2007] describes it's objectives as being "*to build a safe, just and tolerant society through the application of science and technology*". Their work includes: improving video and CCTV operations; improving the imaging technology that interprets the images collected; introducing and refining the use of biometrics in the registration of asylum seekers, iris recognition for frequent travellers to the UK and the incorporation of digitised images of passport holders' faces into the RFID chip held on the UK passport. The government has also instructed the Ministry of Defence to make their "*gait recognition*" software available for widespread use [Johnston, 2007]. This software analyses how individuals walk and seeks to be able to identify who those individuals are, based on that analysis. The Home Office has also encouraged the use of fingerprinting in pubs and clubs to be extended from the rural pilot area of Yeovil for introduction into bigger cities [Ballard, 2006].

2.5 Educational Influences

Education campaigns aim to highlight the potential problems from personal privacy breaches, giving advice and guidance on how to prevent or avoid those breaches. Within the UK, education campaigns are influenced not only by UK bodies, but also by European bodies. Charitable organisations join with commercial organisations to deliver similar

messages, but with different agendas. This section outlines the main education campaigns that concern protecting personal privacy from the commercial, charitable and political sectors.

The illegal sharing of copyright music is of great concern to the music industry. The BPI, the British record industry trade association has worked in collaboration with ChildNet International in bringing about a campaign to inform parents about the illegality of downloading copyrighted music without paying for it [ChildNet, 2007]. This campaign is aimed primarily at informing parents so that they can prevent their children illegally downloading music. However, there are warnings about the potential for downloading files that may have the appearance of music but have the potential to contain pornography or spyware instead. The reason this comes under consideration for impacting personal privacy, is that many spyware programs seek to collect information about the individual, and infection from spyware was also ranked third in the top 10 security threats outlined in PC Magazine [2007]. The spyware may have malicious intent such as illegal access to financial accounts, use of personal information for identity fraud, or perhaps what might be considered as less malicious, information collected for marketing purposes.

The protection of children has become a major concern, generated perhaps to some extent by the "gross sensationalism" and "crass exploitation" of sex offenders and sex crimes by the media [Clark, 2001]. At the time of writing, Jenkins [2007] has questioned the media frenzy concerning an abducted child in Portugal, stating that the media intrusion into the privacy of the family is unlikely to be beneficial in helping to find the child. Regardless of media motivations in generating this concern, and despite Furedi [2002]

questioning child protection approaches, suggesting that they merely add to a "*misanthropic mood of the time*", it remains true that the protection of children and young people in an digitally connected environment is a necessity. The following section, 2.6, considers the social influences on privacy, illustrating the increasing pressures on young people and children to give out more of their personal information, or to let more people into their private lives. These education campaigns from the children's charities and the law enforcement bodies therefore seek to inform both the young people themselves, and the people who bear the responsibility for their welfare.

In the charitable sector, several of the major childrens' charities have joined together to form the Children's Charities Coalition for Internet Safety. Between them they place educational materials on their websites to inform parents and young people about sharing information. The NCH [2007] choose to make use of television characters Dick and Dom to bring their message across, where the NSPCC [2007] aim their message primarily at the parents and carers of young people.

Across Europe, the Insafe network is a body that coordinates the Internet safety activities across Europe and is supported by the European Commission. Within each country there is a body, referred to as a node, working with Insafe to encourage safe use of the Internet [Insafe, 2007]. Insafe provides a central repository for safety resources, supports the International Association of Internet Hotlines, founded in 1999 under the EC Safer Internet Action Plan, and issues a monthly newsletter detailing Internet safety work being carried out across Europe. At the time of writing, the current UK node is the Cyberspace Research Unit (CRU) at Lancaster who are responsible for setting up the Internet Safety

Zone, and the For Kids, By Kids Online [CRU, 2007].

Home Office activity has not been restricted to the CRU in setting up the Internet Safety Zone. The UK political influence has been felt in the setting up of CEOP, the DirectGovKids website and the Get Safe Online website. CEOP, is the Child Exploitation and Online Protection Centre [CEOP, 2007], and links local police forces with relevant bodies. Their website, www.thinkyouknow.co.uk is aimed at young people and gives advice on the interaction of young people with technology, the design of which is informed by their youth panel. CEOP also has links to the Virtual Global Taskforce, a body that combines resources in investigating global child abuse, and there are also industrial partners who work with CEOP to incorporate safety features into the design of technology. Microsoft for example have have incorporated a "Report Abuse" button within Instant Messenger, Bebo the social networking website have also placed a Report Abuse link. The DirectGovKids website provides online activities, for young people aged between five and eleven, giving tips on how to stay safe online [Direct Gov, 2007]. The Get Safe Online website offers questionnaires to assess online safety consciousness, resources for parents, teachers and young people, and a personal security checklist [Get Safe Online, 2007].

2.6 Social Influences

This section examines how technology affects individuals through the social web, mobile and other communication devices, and the increase in surveillance technologies.

2.6.1 Social Web

The Internet is becoming a more social space with individuals choosing to make use of

web applications that allow them to share their thoughts, feelings, photographs and videos. O'Reilly [2005] described this approach as being a new evolution of the web, giving it the title "*Web 2.0*". Treese [2006] discounts the hype towards Web 2.0, maintaining that what is emerging is an approach where technology is being applied slowly and incrementally to create exploratory innovation, and the slump after the dot com boom makes the current innovations appear more of a paradigm shift than they really are.

Individuals have many collaborative and user-driven sites to choose from, and those mentioned in the discussions that follow are the most common examples at the time of writing. www.go2web20.net collects together the logos of web 2.0 applications, indicating on its display that there are 1153 different applications at 29th April 2007. The unifying feature of web 2.0 applications are the ability for users to create their own content and they fall into two types, the gathering of information either collectively or through collaboration, and the personal site [Lanchester, 2006].

From the personal perspective, individuals can interact with their chosen communities and peer groups in a wide variety of ways, utilising software such as:

- social networking websites, for example MySpace, Bebo or Facebook;
- blogs and online diaries, facilitated by sites such as Blogger.com;
- sharing of photographs and videos, utilising Flickr or YouTube for example.

MySpace launched in 2003 to allow bands to promote their music, because the social networking website of the time, Friendster, did not allow bands to post content there

[Lanchester, 2006]. The social networking websites available are rapidly changing and the Nielsen net ratings for March 2006 and April 2007 illustrate how Bebo and Facebook are vying for top position. The measures taken by Nielsen look at page views and time spent on the website and at the time of writing Bebo was one of the most popular websites with "*kids and teenagers*" [Nielsen, 2006; Nielsen, 2007] .

Online diaries, or blogs, are not restricted to social networking websites, content management systems allow individuals to post their thoughts, photographs and links. An analysis of 15 different blogging applications current in 2005 is found at http://asymptomatic.net/blogbreakdown.htm, and the OJR [2006] analysis lists 8 primary ones. One example of a web application where individuals can upload photographs to be shared by others is Flikr, www.flickr.com. The photographs are annotated by individuals by adding tags and building up a classification of the photographs. YouTube, www.youtube.com, offer a similar service for video clips.

Collaborative sites are seen with wikipedia, del.icio.us, citeulike. Wikipedia is based on the concept of an open encyclopaedia and provides an environment where content can be modified by anybody. This does bring it in for criticism for being unreliable and inaccurate [Melly, 2007]. Del.icio.us, http://del.icio.us/about, is a social bookmarking website where individuals can create a list of favourite websites, categorise them with tags and make them publicly available. Citeulike, www.citeulike.org, provides a very similar experience, but from an academic perspective.

Creating personal content has become easier with the technology available. "Mashups"

allow individuals to create their own content based upon different sources outside of their personal boundaries [Merrill, 2006]; online mapping services offered by Google or Yahoo can be combined with personal markers and can create applications tailored to different domains, as Boulos and Wheeler [2007] explore within the health domain. Yahoo has introduced a service called Yahoo Pipes that allows users to create tailored web applications using a graphical user interface [Cubrilovic, 2007]. This approach has been facilitated with the popularity of websites syndicating their data utilising RSS feeds.

Finally, discussion on the social aspect of the Internet would not be complete without reference to the leisure industry containing virtual worlds and online gaming. Virtual worlds such as Second Life have become very popular with individuals creating their own virtual world and interacting with others, yet having value in the real world [Hof, 2006]. Chen et al [2006] discovered that social interaction between gamers was one of the driving forces behind those who achieved well in the games. These virtual worlds and games have the ability to disseminate large amounts of personal information, if individuals are not careful about what they divulge.

2.6.2 Mobile Communication Devices

Mobile phone usage has seen unprecedented growth in recent years [World Telecommunication/ICT Development Report, 2006]. 77% of 7 – 16 year olds in the UK now own a mobile device [HBOS, 2006] making mobile communications one of the most significant developments in the fields of information and communications technology [Plant 2000]. Mobile devices not only offer basic telephony functionality but come with the ability to record and send images and videos, embedded RFID chips enable purchasing [Warren,

2005] and increasingly have accurate embedded sensors for Global Positioning System (GPS) functionality or digital compasses [Simon et al, 2006].

Interaction with peers can happen through text, email and instant messaging. The mobile phone has become a powerful hand-held computer [Prensky, 2005]. From personal experience, it has been difficult to purchase a mobile phone without a camera. New phones are available with two cameras, one for taking digital photographs and another smaller one for use for use in video calls.

Mobile devices come with a range of connectivity options, Bluetooth along with Wireless (Wi-Fi) connectivity allow for different methods of transfer of images at little or no cost to the owner of phone. To use Bluetooth, two devices must be paired together, Wireless networks can be accessed with varying levels of security. Wireless is becoming popular for use with both mobile devices and home computing. In public spaces wireless hotspots provide ubiquitous wireless Internet access for a fee [Ward, 2006] and within the home environment, wireless is increasingly chosen as the mode of delivery for connecting to the Internet [Rubens, 2007].

Interaction between individuals has not been limited to the Internet, mobile devices are sharing in this approach. New Nokia phones contain LifeBlog software offering the ability to create an online diary whilst on the move. O2 encourage individuals to upload content in return for payment [O2, 2006]. YouTube have launched the facility to access videos from their website using mobile phones [BBC, 2006b].

2.6.3 Aggregating Technologies

Mobile devices and the Internet are combining to bring surveillance capabilities to the ordinary person. Devices that form part of everyday life have become tools for surveillance, mobile phones for example, provide an array of functions turning them into a supervisory tool. Location can be tracked by a third party [Shallcross, 2006]; software can transform a mobile phone into a surveillance camera [Smart Card Group, 2006]; voice analysis software can be used to monitor phone calls and advise on predominant emotions [Power, 2006]; and CCTV cameras can interact with mobile phones [Smith, 2003]. Anxious parents concerned about their children being abducted from the home can purchase children's clothing with RFID chips embedded and place tag readers around the house to detect if the clothing is removed [PhysOrg, 2005]. Sensors are available for the home, tracking people as they move about allowing automatic adjustment of heating and lighting. Increasingly these sensors have the built in ability for remote control through the Internet.

2.7 Conclusion

Every aspect of an individuals' life is likely to be affected in some way by technology and the effect it has on their personal information. Earlier in this section, the dilemmas and issues posed by the conflicting and outdated legal approaches were presented, not to mention the imbalance of power created by a legal approach where only those with sufficient funds are able to resort to legal means for their privacy protection. The commercial world was examined, illustrating how personal information and the manipulation of it is underpinning commercial activity, leading to the tension between providing the convenience which individuals desire, while engendering their trust. The

changes in the political arena were introduced, where public data has become even more easily and widely available through moves to engage the general public with the government through technology. Education campaigns bring with them what appears to be a double edged sword, they seek to inform, or instil more fear, depending on your viewpoint. From the social perspective, the Internet is moving to a forum where giving out personal information is made easier. Convergence with mobile devices allows this approach to be taken irrespective of location. Finally, surveillance technologies are emerging within reach of the individual, no longer in the province of the law enforcement bodies or the private investigators.

This myriad of different influences impinging upon personal privacy for the individual show there is an intersection that should be investigated further. The following chapter explores in more detail the intersection between personal data and Internet connectivity from the perspective of the potential for harm, examining what the potential is and the current solutions offered to minimise that potential for harm.

3 Potential for Harm

This chapter examines the current body of knowledge about the protection of personal privacy by considering the potential consequences from privacy breaches. The separate risk areas of harm are considered which are: financial loss; changed behaviour; and mental or physical harm. Each category is discussed below, presenting the manifestation of potential risks and the current body of thought. The chapter concludes with a critique of existing solutions and concludes with the emergent research objectives.

The release of personal information in itself is not a problem, it is the potential for, or the fear of, abuse of that information that causes concern. The consequences can be identified in terms of risks, the manifestation of which can be divided into three main categories which carry some overlap.

3.1 Financial Loss

Financial loss for the individual is most usually the result of some form of fraudulent activity. Fraudulent activity can occur at different levels: the individual may be targeted directly; their workplace may be targeted thus leading to a detrimental effect on them, perhaps losing their job if redundancies had to be made or the business went bankrupt; or their investments may be targeted, leading to severe financial impact at a later date, (for example a pension fund may be defrauded leaving no money to pay out on retirement). While it is acknowledged that all have a potentially serious impact, the scope of this section will be to reflect the focus of the research and concentrate on the individual. Therefore discussion is confined to financial loss when the individual is targeted directly.

The individual can be targeted directly in a number of ways:

- Identity Theft, or impersonation fraud, where the identity of an individual is misused to obtain goods or services;
- fraudulent transactions on credit card or bank account; where the individual falls prey to a scam delivered through spam emails.

There is an argument that using the term "Identity Theft" is misleading, Toby Stevens, chair of the BCS Information Privacy Expert panel, states that there is no such thing as Identity Theft, merely the misappropriation or abusive use of identifiable information [Stevens, 2007].

CIFAS is the UK fraud prevention service comprising an association of two hundred and seventy members from across the financial sector [CIFAS, 2007]. One of the steps they take on detecting any attempt at identity fraud, is to record a warning against the address of the individual. The effect of this warning is to slow any credit application process to ensure that more detailed and thorough checking can be carried out. Whilst the Fraud Advisory Panel [2006] reported a hundred thousand victims of identity fraud each year, CIFAS report that the number of victims has only increased by 19.91% from fifty thousand reported in 2004 [CIFAS, 2007]. The number of attempted frauds has risen, but so too has the number of frauds detected prior to the individual being affected.

Situated in this climate of concern surrounding identity fraud, a number of identity fraud insurance services have emerged. Services are available for the individual to monitor their

credit reports, and range from the simple credit file checking services provided by the likes of www.checkmyfile.com to the more value added approach demonstrated by Data Patrol from www.garlik.com. Data patrol sets out to provide a more comprehensive view of available personal data, aggregating different sources of information about the individual. Public records are combined with credit reports and information discovered through the Internet. However, on investigation, this does appear to have the limitation that it only reports on instances where the individual's name has appeared on a webpage.

Financial loss is just one of the aspects of Identity Theft, it has the potential to lead to difficulty in obtaining loans, mortgages, security clearance, promotion, employment and in some cases has led to wrongful arrest. The anxiety created by the experience has been linked to psychological harm [Fraud Advisory Panel, 2006]. Within the US estimates of the time taken for an individual to repair Identity Theft damage range from 60 hours to 400 hours, with some individuals spending a lot of money on repair activities and having to deal with between 20 to 30 lenders or institutions [Solove, 2003]. Within the UK, CIFAS record the time to be much less at between 3 to 48 hours [CIFAS, 2007a]. These figures represent the detected loss where Identity fraud has been discovered and a measure is able to taken of tangible costs. The misuse of credit cards is often discovered quickly and credit card companies will report on losses as a direct result of lost or stolen cards or cardholder not present frauds [Newman and McNally, 2005]. There are other aspects of Identity fraud that are not accounted for because it is not reported and hence the figures do not illustrate the true scale [Guardian, 2006]. From the perspective of the individual there are a number of issues to face [Newman and McNally, 2005]:

- Older or less educated individuals less likely to discover this type of fraud.
- Fraud involving children may not come to light until they start to become credit active.
- Prices may increase as companies seek to offset security costs.
- Personal data may be sold on by companies to offset security costs.
- Identity fraud where new accounts are opened may take place where the individual is never likely to encounter them.

The manifestation of Identity Theft is seen by Solove [2003] to be the result of an "Architecture of vulnerability". His argument is that because information flow is seen to be critical in the shaping of society, the design and structure of those flows affect the fundamental practices within that society. Individuals are therefore being placed at risk by the structure of the information flow, but are powerless to mitigate any of those risks. In later literature, Solove [2006] describes the different activities that put individuals at greater risk of Identity Theft, one of the main issues being the insecurity of personal information that has been identified and aggregated. This insecurity arises from security lapses, abuses and illicit use of personal information. At the time of writing, the issue of divulging large quantities of personal information to household surveys has been highlighted. In return for a small box of Thornton's chocolates, the Household Insight Survey will collect your name, address, marital status, credit card activity details, partners date of birth, occupation, children's date of birth and gender. The instructions on the questionnaire are to place the completed questionnaire inside a highly visible red bag and leave it on the

doorstep by 9am the following morning. The irony of the situation has already been highlighted by Bibby [2007] in that Experian, one of the major credit reference agencies is a recipient of the information. Experian already offer a service for individuals to check their credit reports for evidence of activity related to Identity Theft at www.creditexpert.co.uk.

Identity Theft is not a new crime, this type of fraud has existed for many years, however the wealth of information available through the Internet has created new opportunities for fraudulent behaviour [Tavani, 2007]. The Fraud Advisory Panel identified virtual communities as contributing to Identity Theft, allowing new opportunities for money laundering through false online identities [2007a]. The design of the new UK passports has raised concern regarding the potential for Identity Theft. New passports contain RFID chips embedded into them containing identity information. The passports utilise the International Civil Aviation Organization (ICAO) standard security architecture that has been adopted worldwide for machine-readable passports. The concerns centre around the ease in which personal information can be obtained. One investigation carried out by Kirk [2007] utilised known personal information to unlock the data held on the RFID chip, which had been read through a sealed envelope. Herrigel and Jian [2006] also investigated the ICAO standard for the potential for Identity Theft and proposed that high capacity digital watermarking be utilised as a solution.

Anderson [2006] has identified categories of individuals who are likely to be most at risk from Identity Theft:

- those on higher incomes;

- younger consumers; and
- women.

These categories are further divided by consideration of contributory factors:

- number of non-cash accounts;
- intensity of use of accounts;
- where business is conducted; and
- precautions taken.

Medical Identity Theft is reported in the US as being where the identity of an individual has been used to obtain medical services or goods or make false claims on insurance for medical services [Dixon, 2006; Security Views, 2006]. Whilst this has a more serious impact within the US, the effects could just as easily be felt here in the UK. Within the UK there are healthcare insurance services offered by the likes of BUPA that allow an individual to have preferential or quicker healthcare bypassing NHS waiting lists. With the advent of the electronic patient record, erroneous or false entries on that record could lead to misdiagnosis, incorrect medical treatments or cancelled life insurance [Dixon, 2006]. The problems faced by individuals with the centralisation of their medical records is one highlighted by the campaign, The Big Opt Out [2006]. However, they make the point on their website that Accident and Emergency centres across the UK have procedures for giving treatment to an individual presenting themselves, and looking up a centralised medical record is not currently one of those procedures. At the time of writing, the accidental loss of data is causing concern for individuals. There has been the accidental

loss of patient data, which has arisen quickly after the accidental loss of personal details for those in receipt of child benefit by the Inland Revenue [BBC, 2007b]. Eight trusts have been reported to have lost a hundred and sixty-eight thousand patient details [BBC, 2007a]

An individual may be affected by fraudulent financial transactions occurring on their bank or credit card accounts. Since 1 April 2007 consumers no longer report potential fraud to the police, they have to notify their bank of any transactions they have not authorised allowing the banks to decide whether or not the fraud is reported to the police [Howard, 2007]. Small businesses are increasingly being targeted by fraudulent activity, and primarily bear the cost. Once the fraudulent transaction has been identified by the consumer, the amount is refunded to them. However the small business is charged a fee for the transaction and the money reclaimed from them. Tedeschi [2006] argues that these smaller retailers are being targeted because the larger retailers are able to invest heavily in anti-fraud measures.

Surveillance technologies increase the sophistication in observing an individual interacting with a cash withdrawal machine. Skimming and cloning of bank cards along with recording the keys pressed to enter the four digit PIN number can easily be carried out without the individual being aware that it is happening. With the information gleaned, small and irregular withdrawals are made from the bank accounts so that the alert to the fraud is minimised [Thomson, 2005]. With the advent of Chip and PIN, where retailers request the individual to enter their PIN number to authenticate the transaction, the reporting of this type of card fraud has decreased [APACS, 2007]. Gathering enough account information

to perpetrate online banking fraud is not limited to the interactions with the cash machines, increasingly individuals are being targeted through approaches such as: [Furnell, 2005]

- phishing, plausible but false emails. Over one hundred and ninety-six thousand unique phishing emails were identified in the last part of 2006 [Symantec, 2007].;
- spyware, as reported earlier, was deemed to rank third in the PC Magazine's [2007] top ten, it is also reported by Sophos [2007] to be the second biggest problem for businesses.
- malware, a deliberate program designed to damage the users machine is now targeting the individual and Sophos [2007] have detected over forty-one thousand new pieces of malware during 2006; and
- hacking, not such a wide scale problem, only sixty-seven incidents in 2007 reported to the Web Hacking Incidents Database [Web Application Security Consortium ,2007]..

Consumer devices now add to the potential for fraud with harm arising from acquiring identifiers and authentication by intercepting usernames and passwords. Transactions can now be initiated by somebody other than the authorised user, for example seen in the transfer of funds. Transactions undertaken by the authorised user could be interfered with, for example by diverting legitimate transactions. The consumer device may be utilised to perpetrate fraud on a third party, using the device as a staging post within a chain for transaction laundering [Clarke, 2007].

Phishing, where an email lures an individual into giving out sensitive personal information

by purporting to be from a trusted institution, has been described as a form of social engineering [Thomson, 2005] or online Identity Theft [Kirda and Kruegel, 2006]. The Symantec [2007] figures quoted above illustrated how large numbers of phishing emails can be sent, the cost of which is minimal. Therefore only a small percentage is required where individuals are taken in by the phishing scam to yield enough of a return. Government websites, such as getsafeonline.org.uk, banking websites, and the banking industry website, banksafeonline.org.uk, seek to raise awareness of the dangers of responding to phishing emails. The Bank of Ireland announced that they would not compensate individuals for losses incurred as a result of responding to phishing emails, thus emphasising the responsibility that individuals have themselves for keeping their personal details secure [O'Brien, 2006]. Emails are evolving from the mass distributed, blanket email, sent to everybody in the hope that somebody would respond, to the more targeted approach which has been termed "spear-phishing". Personal information is harvested from social networking websites, allowing for passwords to be calculated [Simmons, 2007] and individuals, usually with high incomes, targeted [Kelly, 2007].

As mentioned above, phishing emails can be seen as one technique exercised by the social engineering approach to dishonestly obtaining personal information. Social engineering has been described by Mitnick et al [2002] as exploiting the weakest link in a system, that weakest link being the individual who falls prey to clever manipulation of the basic human tendency to trust [Granger, 2001]. One court case illustrated how social engineering techniques were utilised by private investigators to uncover financial details of the individuals being investigated [Leigh and Evans, 2006]. Social engineering has been identified by Chen et al [2005] as being one of the major criminal means for online games

crime. In an analysis of games crime cases in 2002 Identity Theft was 43.4% and social engineering 43.9%. The human element within any IT system has been recognised as being one of the causes of serious risk. With the increase in social engineering attempts to perpetrate fraud, addressing this risk through good organisational structures, management and leadership along with user awareness and commitment has become essential [von Solms, 2006].

3.2 Altered Behaviour

The psychological need for privacy, combined with a belief in privacy rights has been seen to affect online privacy concerns [Yao et al, 2007]. This section explores the sociological literature which considers the effects that privacy has on the behaviour of individuals, and indeed upon their experiences of others' behaviour, when there is a lack of privacy. Discriminatory experiences, repression of thought, observation or surveillance, decreased trust, vulnerability and perceptions of risk are all noted consequences of the lack of privacy. These concepts are explored in more detail below.

Privacy has been identified as important for avoiding discriminatory situations, for example, Solove [2004] has defined privacy in terms of the desire to prevent being misjudged out of context. Wainwright [2007] highlights this issue in a media report, CCTV cameras with speakers were used and a wrong accusation was made. In this situation, a mother was publicly berated by a CCTV operator for dropping litter, when in fact she was only placing litter on the tray at the bottom of her child's pushchair. The incident later appeared on the television news as an example of the new style CCTV cameras combined with speakers being utilised to address antisocial behaviour. Concern about being

misunderstood, and the potential for being judged purely by a gender stereotype, has also been described by Miller and Arnold [2001] in the situation where some female academics choose not to post photographs alongside professional details. A dilemma was described where individuals felt they had to choose between exposing themselves to prejudice or appearing friendly and validating their academic credentials. Problems for young people have been identified where the trails of information they leave online are aggregated and categorised, leading to discrimination in terms of high health insurance, refusal of credit or employment [Leenes and Koops, 2005; RAE, 2007]. Searle [2006] noted that increasingly surveillance and data collection technologies were being utilised in recruitment practices that potentially perpetuated the discrimination of already marginalised groups. The imbalance of power was bought about by assembling data on the job seeker combined with tools for recruiters.

The importance of privacy in protecting freedom of thought, allowing individuals the freedom to hold political, religious and personal viewpoints, is emphasised by Cavoukian and Tapscott [1997]. This freedom is described as being an important element in moving informed debate forward, which in turn benefits democracy and society [Garfinkel, 2000]. Within westernised society democracy and freedom of speech is highly prized, however, within other nations this is not the case. Kunzru [2007] highlights how information from Yahoo to the Chinese Government led to the conviction of a journalist for posting criticism of the Chinese Government, and prison sentences were issued for those participating in a pro-democracy discussion forum. The Electronic Frontier Foundation is involved in a project (http://www.chillingeffects.org/) to monitor how many individuals and companies are using intellectual property rights and other laws to control what other online users post,

thus restricting an apparent freedom of speech. There are many dilemmas with respect to allowing individuals the freedom to articulate their views. Privacy can protect those who seek to spread hatred through racism or seek to harm others, and there needs to be a balance between protecting the whistle-blower or the dissident against hiding the bigot or the racist. The lack of privacy gives rise to a lack of autonomy of the individual, an important element in the ability to fulfil the role of citizen and consumer [Raab, 2004].

Observing individuals has been seen to alter behaviour - mental health problems, paranoia, anti-social behaviour have been cited as examples of the effects [Cavoukian and Tapscott, 1997; Feenberg, 1999]. Anti-social behaviour has been cited by Solove [2003] as a result of covert collection of personal data resulting in individuals becoming disillusioned and disempowered. The Royal Academy of Engineering [2007] "Report on the Dilemmas of Privacy and Surveillance", expressed concern that the greater collection and storage of personal data has the potential to significantly decrease trust.

Trust is an important aspect to E-Commerce, more business is generated as individuals trust their transactions to be handled correctly [Guerra et al, 2003]. However, whilst 80% of individuals desire the benefits of personalised content, such as seen with Amazon, they are not prepared to divulge large amounts of information to obtain it [Hochhauser, 2000; Kerner, 2005]. In 2003, the European Commission [2003] survey discovered that two thirds of individuals were concerned about giving out personal information. This concern translates itself into individuals not making as much use of the E-Commerce opportunities as might be otherwise found. Sinclaire et al [2006] found that companies without an offline presence, trading solely online, were viewed as more of a risk than those who had both

online and offline presence. 65% of the respondents believed that using the Internet would lead to personal privacy problems. Hirsch [2005] has compared the privacy approaches for business to those of environmental damage. The business does not bear the cost of the privacy invasion, but if privacy is not managed properly business activity could destroy the resource, that being the information of individuals.

E-Commerce is not the only area seen to be affected, privacy concerns have had a detrimental effect on healthcare. In one area, withholding consent to use personal data has had a detrimental effect on research, especially when involving children or vulnerable adults [Arnold et al, 1995]. Zeps et al [2007] have attempted to overcome these barriers to consent, by making use of ethics committees to ensure the proper privacy protection of individuals, and were then able to conduct beneficial cancer research. In another area of healthcare, concerns with regard to confidentiality have been found to discourage particularly vulnerable teenagers from seeking the healthcare they need [Lehrer et al, 2007]. This point has been emphasised by the The Big Opt Out [2006] campaign who highlight Anderson's [2006] concern about the integration of the NHS Care Record Scheme into other governmental databases. The concern voiced by Anderson [2006] was that this integration of databases would not just stigmatise young people, but there was the potential that vulnerable individuals would be bullied, or coerced, into divulging their passwords so that others could access their healthspace records. Concern was also raised about making the social engineering approach mentioned above, or "pretexting" easier. It would need only one NHS employee with access to the central records to give out information.

Vulnerability was mentioned earlier connected with financial loss [Solove, 2004], and is a term that can have multiple connotations in different contexts. From the perspective of altered behaviour, vulnerability is viewed as the propensity for an individual to be harmed or their perceived risk of harm. Using this approach to vulnerability a strong link to the disclosure of personal information has been made [Dinev and Hart, 2004]. The more information disclosed, the more vulnerable an individual becomes [Margulis, 1977]. For example, individuals on low incomes were considered to be more easily influenced into spending their money, by the focused marketing from companies using personal information [Valongo, 2000]. Another approach taken by Alwang et al [2002] decomposed vulnerability into a chain, illustrated below in Figure 2. Vulnerability is considered in terms of risk, combined with the ability to manage the risk, and the welfare implications if the risk is not, or cannot, be managed.

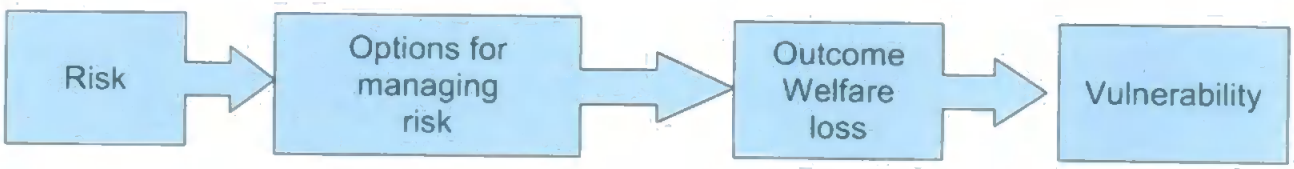


Figure 2: Chain of elements illustrating vulnerability.

Utilising risk, and the ability to control it, as central tenets of vulnerability is not without controversy. Raab and Bennett [1998] reasoned that controlling risks to privacy would address social inequalities whereby some individuals enjoy large amounts of privacy protection, leaving others without any. However, whilst risk avoidance and risk management are gaining increased kudos, there are detrimental effects. Larose and Rifon [2007] discovered that increased privacy warnings generated a heightened state of fear of risk in individuals. Concerns about risks from terrorism and paedophilia have led to

mandatory state access to communications [Kunzro, 2007], along with intrusions through mass surveillance. This echoes the observations that Schwartz [1999] made when stating that privacy invasion would spiral out of control as the majority of individuals passively accept privacy invasion as the norm. Indeed, technology has been described as naturally privacy invasive [Cranor and Garfinkel, 2005; Raab, 2004; Hansen & Kraseman, 2005] and as such is often demonised [Raab, 2004]. Furedi [2002] criticises the approach of avoiding or managing risks, whereby fear of affecting the future by detrimental actions now is combined with a fear of danger, thus making risks appear to be unbounded.

Affecting the behaviour of individuals, however, could be seen in more positive terms. Drive Diagnostics [2006] provide a case study where drivers were given feedback information about their driving via in-car sensors collecting information about their manoeuvres. This case study illustrated the activities of fleet drivers and the impact of monitoring. One media source [Massey, 2005] chose to highlight the device potential for monitoring teenage drivers, a high risk group [Safer Motoring, 2006], which does give rise to consideration as to how this might affect the family dynamics and trust levels between parent and child.

3.3 Mental or Physical Harm

It is irrelevant whether or not the fear of harm is greater than the reality, as Furedi [2002] suggests. What remains is that a significant number of individuals experience mental or physical harm because of the abuse of personal information. This section examines how that abuse of personal information might manifest itself in terms of mental or physical harm. Harm is discussed below in four distinct areas of classification:

- bullying;
- stalking;
- grooming; and
- mental distress.

With the interconnected nature of young people, bullying is moving online [Li, 2007; Ybarra et al, 2006] and to the mobile phone [Charlton et al, 2002]. The tools utilised for bullying come with access to emails, text messaging, discussion boards, and social networks. Bolman [2006] found that most online bullying, often termed "*cyberbullying*", was carried out by teasing, talking or whispering, ignoring, making accusations and hacking. Cyberbullying intensified the victims experience because of the levels of anonymity the bully could hide behind, the large audience, the way the effects spread very quickly and the difficulty in removing the offensive information. Other manifestations of cyberbullying include harassment, intimidation and impersonating others online [Chisholm, 2006]. Bullying is not confined to the realm of young people, an analysis of workplace emails and other communication media discovered a considerable level of bullying within the workplace. From the work perspective, it led to demoralised, anxious employees with low performance who were seriously considering leaving [Baruch, 2005]. Mobile phones have facilitated an increase in harassment with text stalking cases reaching one million per year with 5,640 prosecutions in the UK under harassment legislation introduced in 1997 [Goodchild and Heathcote, 2005]. Statistics from WHOA [2005] show that 40% of harassment started through email and progressed through to the use of message boards, instant messaging, websites and chat facilities.

Mullen [2006] defines stalking as a common problem, usually occurring as a result of some form of psychiatric disorder in the perpetrator and leading to psychological and social damage in the individual experiencing the stalking. Bocij [2004a] disagrees with Mullen about the mental health issues of the perpetrator, suggesting that cyberstalking cannot be classified as just an extension of offline stalking behaviour, because the victim is not always known to the cyberstalker. Cyberstalking involves a variety of behaviours ranging from posting offensive messages to physical attacks and often involves some form of personal data collection from the Internet [Bocij, 2004b]. The most common situations of stalking however, occur when an intimate relationship goes wrong [Spitzberg and Hoobler, 2002] with ex-partners being the number one category of stalkers [Goodchild and Heathcote, 2005]. Increasingly technology is being utilised to carry out tracking, monitoring of individuals is facilitated by the use of caller identity, GPS devices and high resolution web cameras [Southworth, 2005]. A search on Google with the term "track spouse" revealed a multitude of spyware, email scanners and other products primarily aimed at the American market. The website www.trackershack.co.uk offers a large number of tracking devices and spy products to the UK market. Mobile phone tracking, GPS devices and voice detection software has also been promoted as a method of tracking an unfaithful spouse [Power, 2006].

A predatory sexual attack involves an extended period of targeting and grooming, during which the potential abuser attempts to identify and ingratiate themself with the person who will eventually become the victim [Briggs et al, 1998]. During this period, which may include such predatory behaviour as stalking, the abusers self-appointed task is facilitated

by the ready availability of personal information. The growth of information posted on social networking websites has caused alarm with those working in the field of investigating paedophilia, suggesting that the environment gives rise to "new forms of social deviance and criminality" [Brennan, 2006]. Lewis [2006] gives a figure quoted from the police that estimated that "50,000 predators were online at any one time". There is a dichotomy here between the divulging of personal information and the apparent anonymity that the Internet provides for the sexual exploitation of women and children. For those who make use of the global sex industry, supportive communities justify and legitimise actions [Hughes, 2003]. Mitchell et al [2005] find that abusers who make use of the Internet to further their crimes are just as likely to be from the same family or acquaintances, so emphasising that the stranger-danger message is not entirely relevant [Rickert and Ryan, 2007]. In addition, as is emphasised by the CEOP website, www.thinkUknow.co.uk, the virtual environment created by the use of nicknames and avatars means that abusers are able to portray themselves as something they are not, often a younger person. Livingstone [2003] emphasised how public concern for children not only complicates any research in that area, but also centres on unwanted sexual contact. Mitchell et al [2007] have recently carried out a survey that illustrated a significant decline in the reporting of unwanted sexual solicitation, suggesting that this is not as prevalent as the media might have the public believe. Whilst unwanted sexual approaches may be in decline, the point should be made that for those that do experience them, it can cause tremendous mental distress [Finkelor et al, 2003; Ybarra et al, 2004].

Mental distress can be seen with any of the previous harm activities, but special mention here is made with consideration to how release of personal information is being utilised in

terms of abusive behaviour. No one theory of domestic violence has unequivocal support, but treatment programs are based on the power and control model of abuse [Minesota Program Development, 2006], a model that has proved to be one of the most effective methodologies for addressing abusive behaviour [Shephard, 2005]. This model, illustrated below in Figure 3, is based on eight behaviours:

1. intimidation. Fear is generated through the use of looks, actions, gestures, vandalism to property or displaying weapons;
2. emotional abuse. Where comments are made to make the Survivor feel bad about themself, playing of mind games, use of humiliation and generating feelings of guilt;
3. isolation. Control is exhibited over what the Survivor does, who they see and talk to, limiting outside movements and using jealousy to justify the actions;
4. minimizing, denying and blaming. This approach makes light of any abuse and not taking concerns about it seriously. It also includes shifting the blame for the abusive behaviour, suggesting that the Survivor caused it;
5. using children. Children are used to create emotional feelings of guilt, they are used to relay messages and the right of access is used to cause harassment. Threats are made to take children away.;
6. male privilege. This involves treating the Survivor as a servant, ensuring they are not part of any major decisions and conforms to stereotypical gender roles;
7. economic abuse prevents the Survivor from obtaining paid employment, creates the situation where money has to be requested from perpetrator and denying access to the family income; and
8. coercion and threats. This includes making or carrying out threats to harm or hurt

not just the Survivor, but also includes suicide threats. Coercion includes manipulating the Survivor's behaviour so that they drop any charges or are party to illegal acts.

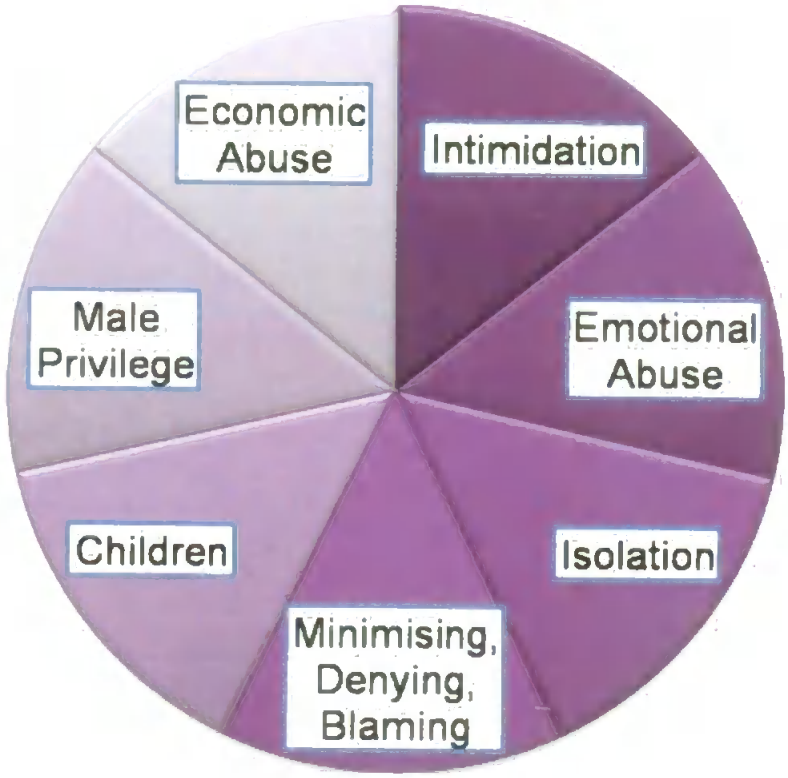


Figure 3: Power and Control Wheel, [Minnesota Program Development, 2006]

These control tactics, in combination with violence, maintain power and control over women [Yllo, 1993]. Beeble et al [2007] point out that abusive men will manipulate the children of a relationship to continue the abusive behaviour, even when a relationship has ended. In this type of situation, location based tracking using mobile phones can cause serious harm. Women are most at risk at the point when they flee from an abusive relationship [WAFE, 2002]. At this point, their physical location and personal information must be kept secret to protect them from further harm. However, there is now a concern

that should a child of the relationship be given a mobile phone which has had the location tracking service set up, any security arrangements made could be compromised.

3.4 Solutions

This section first offers a critique of the technological approaches available, and concludes with a discussion on the management of the risks described above. The tools available for an individual to take a proactive, rather than passive, approach to protecting their privacy are examined, along with the elements involved in the creation of those tools and solutions. Information system security is currently a huge growth area as businesses need to safeguard the data they hold to remain competitive, to comply with the regulations and to engender consumer confidence. Whilst these business approaches do have an effect on the individual, they are only touched upon briefly to illustrate the discussion about the development of tools and solutions, and are therefore on the periphery of the scope of this research.

There is a wide range of software for downloading that claims to protect an individuals' privacy. The Electronic Privacy Information Centre (EPIC) www.epic.org offers a list of links to tools that include the following categories:

- email utilities;
- Internet utilities;
- file erasing; and
- encryption.

Many of these tools are aimed at those who are technically very aware and address some quite narrow issues. There are limitations to the approach whereby end users are responsible for making an explicit choice of the technology to protect their privacy. Furnell [2005], for example, has voiced concern over whether security technologies would be used properly, and whether users would understand and be aware of threats. 72% of individuals in 2003 were found to have not heard of privacy solutions [EU, 2003], and certainly rules and monitoring have been found to be unpopular [Livingstone and Bober, 2005]. There is also the balance to be had between enforcing laws and freedom for the individual [Federrath, 2005].

Identity and the management of it are becoming important issues that are likely to have an impact on the individual. The European Commission is funding research projects into identity and privacy with both the FIDIS and the PRIME projects [Fidis, 2007; Prime, 2007]. FIDIS brings together a multidisciplinary consortium of 24 partners from across Europe, PRIME is a research project creating a prototype privacy and identity management system. Within the UK there has been much discussion and criticism about the introduction of Identity Cards [Blunkett, 2004; eGov Monitor, 2005; No2ID, 2007], however, the requirement for individuals to be able to prove who they are, whether they are unique upon the system and whether they are genuine, remains [Stevens, 2007].

Privacy policies have been determined as an important element of being able to interpret and evaluate how a business will process or forward personal data collected through their website [Nelson, 1998], with classification schemes [Jarvinen et al, 2002] and formats such as the the W3C Platform for Privacy Preferences (P3P) [W3C, 2006] being proposed.

The P3P is a standard for expressing privacy policies in XML format, the benefit of which is that automated tools can be designed to assist the end user in interpreting the website privacy policies. The W3C maintains a list of current implementations on their website which currently illustrates that choices for the individual are limited. For those utilising Internet Explorer, there is the Privacy Bird [2005], for those making use of Mozilla, there is the Privacy Fox [2007]. A development not yet in the public domain, is the use of P3P privacy policies and agents to reason with them. These form part of an architecture and model created by Jutla et al [2004], which proposes to allow more user control to generate online trust and privacy protection. The use of agents to interpret these policies has been criticised for the subjective approach they bring, the agents would interpret the policies based upon the developers perspective and bias. Cranor and Reidenberg [2002] made the criticism that this subjective approach to decision making using P3P policies leads to ambiguity, confusion and legal uncertainty to the situation.

Other approaches an individual can choose to protect their privacy involve making use of software such as Bugnosis [Martin, 2005] or any number of privacy software products that concentrate on deleting personal files from the hard drive. Bugnosis is software that identifies a particular type of anti-privacy practice and it's aim is to contribute to raising an awareness of how individuals are monitored when visiting websites. Other software packages claim to delete personal data files and erase activity which can be quite useful if the hard drive of the computer is to be disposed of. However, this is not always a relevant approach to take and as Geiger and Cranor [2005] outline in their evaluation of these types of software, the approach taken often leaves behind some traces of activity. Other approaches include a privacy infrastructure that alerts an individual as soon as a

photograph of themselves is distributed [Deng et al, 2006]; and the Identity Angel [Sweeney, 2006] which crawls the web looking for public information held about them.

Privacy Enhancing Technologies (PETs) are designed to allow individuals to take action to protect their own privacy [Stalder, 2002]. PETs seek to minimise or eliminate the collection of identifiable data, protect user identities by using anonymity, pseudonymity, unlinkability and unobservability through the P3P privacy tools mentioned above, and digital watermarking approaches to detect where data has been copied [HISPEC, 2002; Burkett, 1997]. The use of PETs is heavily influenced by a complex relationship between market forces, consumer pressure, education and government sponsorship [Bennett, 1997]. Goldberg [2003] in a reflection on how PETs had evolved over a 5 year time span, observed their lack of progress and that many of the applications of privacy were social, not technical issues. Therefore there needed to be an increase in the social and technical constructs combined. The criticism of PETs has been made that they: disconnect the link between action and consequence; their requirements are very narrow [Stalder, 2002]; they legitimise the collection of personal data; and rely too much on the principle of consent from the individual. In a situation where an individual is not able to make any other realistic choices, this can lead to an imbalance of power between those offering the terms and those having to accept them. The interaction of PETs within the system causes an issue, especially if high overheads are created in their use. High overheads can lead to a situation where it is decided that the PET is not worth making use of. The inflexibility is also an issue, in some circumstances individuals may wish to be recognised, but not in others. For example, individuals who wish to make use of social networking websites want to share their information with specific people, but not others. Therefore, the design of

PETs needs to involve the people that it seeks to protect, to ensure their needs are met [Burkett, 1997]. The requirement to work with legal, cultural and social conditions is echoed by Raab [2004]. Good privacy protection is described in terms of a toolkit which can be customised for individuals, an important element given that different individuals have diverse privacy rankings for items depending upon their context [Hawkey and Inkpen, 2006].

Privacy Aware Technologies (PATs) are designed, developed and deployed with privacy as a strong influence throughout but are not direct privacy solutions in themselves. The RAE [2007] proposes that anonymity be built in to technological advances so that they are not automatically linked to an individual. Anonymity is proposed as a solution to addressing location privacy risks with mobile communications [Grutesar and Grunwald, 2003]. In other fields, research has been carried out to assess data files to measure a risk of confidentiality breach. The algorithm involved considers how easily the individual could be re-identified through triangulation and information linkage [Howe et al, 2007].

For those creating software solutions, different approaches to privacy have been proposed. The concern over ubiquitous computing, where sensors monitor and collect personal information [Langheinrich, 2002], has prompted a set of European design guidelines which focus upon specific issues surrounding data collection [Lahlou and Jegou, 2005]. Privacy Interface Analysis is suggested for designing the interface to a privacy enhanced application or service [Patrick and Kenny, 2003]. Consideration of the effects of new technologies can be assessed using Ethical Technological Assessment, an approach used to identify the adverse effects of new technologies [Palm and Hansson,

2006] and Privacy Impact Assessment (PIA) has become an important element to understand the flow of personal data through a system, along with an analysis on how that data is handled. PIA has been linked directly to risk assessment [OMB, 2003] which echoes the argument by Raab [2003] that risk assessment should be a central tenet to privacy protection, not because of the actual identification of risks, but in the way that the process of determining those risks is beneficial. This approach allows for any adverse actual or potential effects on individual privacy to be mitigated.

Privacy has been seen to be a balance of conflicts and can be observed in the balance between protecting those who should be protected and detecting those who are intent on harm. Analysing the conflicts involved and balancing the interests is an approach suggested by Chik [2005] and is essentially a risk management approach. However, the risk management approach is a complex one, with the assessment of risk being highly subjective. Risk assessments are usually carried out by experts within a field to consider specific hazards and give proposals on how to minimise or remove the identified risks. However, problems arise in a number of ways. Internet devices, their uses and impacts pose many different hazards in many different situations. Problems also arise when different experts attribute different meanings and weightings to risks [Kemshall and McIvor, 2004]. Disparate social groups are affected in different ways and require different assumptions to be made. Simplistic risk assessment techniques may not give a realistic assessment of the situation [Lefley, 1997] and the best approach utilises a combination of expert knowledge, objective calculation of risk and subjective views of individuals [Raab, 1998].

Managing the risk of harm to individuals can be considered more alarming when viewed in the light of the Internet being a more social space. Concern about young people and children is such that the European Commission [2006] brings together European countries to work together for a safer Internet environment for children, and the UK Home Office initiated the Child Exploitation and Online Protection Centre [CEOP, 2007] referred to in chapter 2. To address concerns about the risks of new technologies raised by those who educate young people, Becta [2006] suggested that e-safety guidance be incorporated into child protection policies and that each local authority have an e-safety strategy implemented by an e-safety lead [Becta, 2006].

Finally, consideration of the potential for harm would not be complete without examining the issue of the Semantic Web. The Semantic Web began as a vision proposed by Berners-Lee [2000] where carefully described data using RDF, related through ontologies, would provide a powerful ability to combine disparate pieces of information and reuse data already held [Updegrove, 2005]. This approach would remove the current issues of interoperability whereby data held in a sound or image file is not easily accessible. By removing the barriers to interoperability, and streamlining the interchange of data [Passin, 2005], Internet applications using reasoning tools would be able to combine many different sources of information, quickly and easily.

Earlier in this chapter, discussions have surrounded how abuse of information is facilitated when different pieces of information are combined. The decentralisation of personal information lends itself to a simple form of privacy, the amount of effort expended to combine that information will often outweigh the benefits gained when the information is

combined. However, the Semantic Web has the potential to combine these pieces of information quickly and dynamically, and as such has the potential to cause privacy problems [Fildes, 2006; Muncaster, 2006]. For example, search queries, bookmarks, favourites and websites visited may not give much away on their own. However, combined with personal information, browser identification, location information gathered through a GPS or mobile phone and a portrait of the individual is created.

The Semantic Web is created from a layering of pre-defined standards. The current focus at the top of the layer stack is on trust and repudiation, which does not focus explicitly upon the protection of personal information of the individual. Other privacy approaches concentrate on software or intelligent agents negotiating privacy terms for the individual [Jutla and Bodorik, 2005], however this does not account for the situations where there is an imbalance of power. The collectors of information, in combination with the lack of accountability, have the upper hand [Stalder, 2002], and often there is no alternative but to divulge the information requested [Carins, 2005]. Mounting a challenge to the collection of information requires confidence, self-assurance and an awareness of the relevant legal remedies.

The use of privacy policies is another research approach utilising the Semantic Web [Kim, 2002]. Solove [2004] suggests that policies are often tortuous, difficult to read, and utilise a blanket approach, which has limitations for some individuals under different contexts. The Platform for Privacy Preferences (P3P) standard proposed by the W3C [2006] allows users to make use of automated tools, like the Privacy Bird, to visually express whether website privacy policies match their own requirements [Byers et al, 2004]. A screenshot

illustrating how the Privacy Bird appears in action is shown below in Figure 4, courtesy of www.privacybird.org press releases.

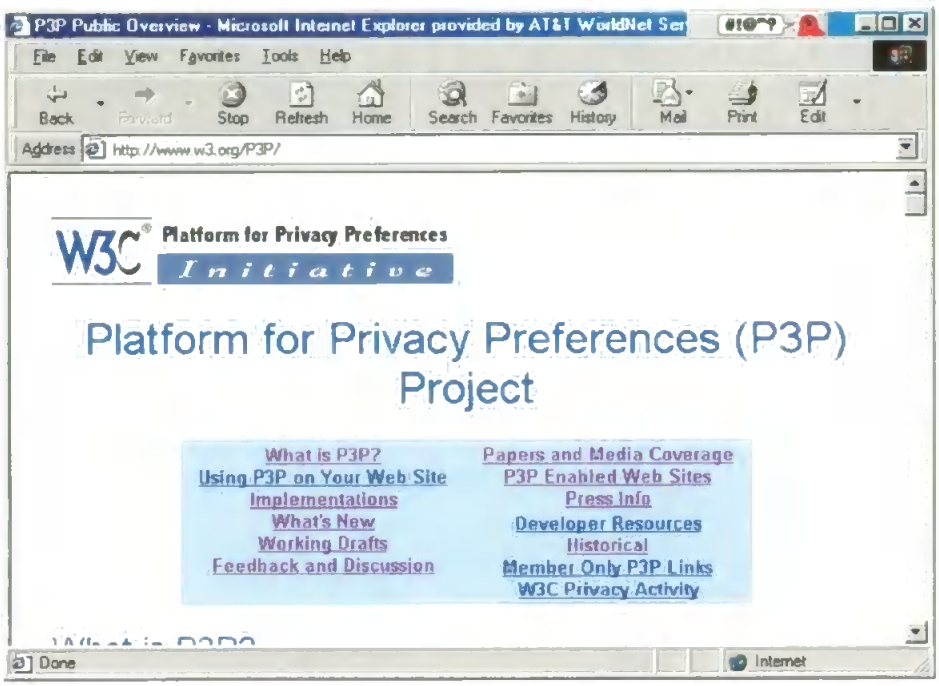


Figure 4: Screen shot of the AT&T Privacy Bird, [http://www.privacybird.org/privacybird-screenshots-020102.ppt]

However, Stalder (2002) argues that this P3P policy initiative encourages the collection of personal information and leads to a false sense of security. Another shortcoming is that users are not necessarily aware of what other privacy approaches might be available [Kolari et al, 2005].

3.5 Conclusion

The separate influences upon personal privacy bring about risks in the three separate areas of financial loss, altered behaviour and actual mental or physical harm. The Internet has facilitated fraudulent activity for misappropriating identity and other techniques have

emerged for gaining access to an individual's funds. The lack of privacy brings about concern surrounding the potential for detrimental psychological effects alongside the potential for discriminatory situations. The concept of vulnerability directly links to the release of personal information and requires an approach whereby risk is directly understood and managed. Bullying, stalking, grooming and mental distress are linked with the interconnected nature of young people along with the use of the Internet for the perpetration of targeting and grooming.

What becomes evident is that privacy enhancing technologies not only have their limitations, but do not address the issues for certain members of society. Some individuals find themselves more at risk of harm than others. The Internet is evolving into a more social medium and there are moves to combine and to infer information in a more effective fashion utilising the Semantic Web. This combination has the potential to manifest some of these elements of harm. It is evident that there is a need to systematically examine how harm arises for specific groups of people, primarily those who may have more privacy risks associated with them and their lifestyle, and then to consider how those risks might be mitigated. The following chapter considers the objectives for this research in more detail and describes how this research proposes to address the problems highlighted in this chapter.

4 Methodology

This chapter begins by considering the importance of an intellectual framework to provide justification for the research methods used, prior to discussing how the research aims determined the selection of the framework. The key methods and underlying theories are reported. The chapter concludes with a reflection and discussion of the methods used.

4.1 Introduction

As observed in the earlier chapters, the potential for harm to the individual arises from a very complex interplay of factors. In order to explore how to reduce that risk of harm, the way the research plan is implemented has to be flexible enough to allow for a view to be taken of this complexity. The methods chosen to carry out the research aims and objectives do not exist in isolation; they form part of an intellectual framework, a set of underlying assumptions and approaches that satisfy the researcher. Choosing appropriate research methods for the aims is therefore very important. Judicious choice will guide the research in providing answers to the research questions [Starks and Trinidad, 2007], but if the research methods are not appropriate, the results will be inconclusive and cannot be applied [Galliers and Land, 1987].

Creating the intellectual framework requires a careful process of consideration, not just of the aims and objectives of the research but also to the role of the researcher. The researcher has a relationship with the aims and objectives, with the research methods and also the participants [Mingers, 2001] and therefore the findings of the research cannot be purely objective. As May [1993] outlines, there is the balance between objective research that ensures that the research findings are not just replications of the researchers opinions

and prejudices, but do, as Hannay [2007] suggests, progress understanding from the observation of a phenomenon to the generating of an explanation of it. Pure objectivity would suggest that the researcher would need to suspend their sense of belonging; they are after all individuals, immersed in society and bring with them a sense of belonging [May, 1993]. Therefore, the methods incorporated into an intellectual framework have to be chosen with care to account for the researcher's subjective values.

The following section begins with a discussion regarding the aims of this piece of research and how those aims shaped which research methods were selected for the intellectual framework. The relevant research methods are introduced and the research space illustrated with a diagram to aid understanding.

4.2 Constructing the Intellectual Framework

As described in the introductory section, 1.2, the first phase of this research requires an examination of the social world in terms of understanding risks. Identifying risks is a highly subjective, human, interpretation of a situation surrounding an individual. Individuals interpret risk in different ways, what is a perceived risk for one person may not be perceived in the same way for another. Context plays a very important role, and chapter 2 illustrated the depth and complexity of the context of personal privacy for an individual by discussing the many interacting influences and factors. Consideration must not just be given to understanding the online, interconnected environment of the Internet, but also towards the offline environment which is just as important [Jones, 1999].

In summary, the research methods utilised must have the ability to address the following requirements:

- Help towards an understanding and exploration of the context in which the research takes place;
- adapt to offline and online context;
- demonstrate an understanding of risks in a format useful for software design.

The research aims indicate a need for a cross-over between:

- software engineering – the need to translate the requirements into a tangible software artefact;
- the information systems domain – the need to understand the interaction between individuals and technology;
- the social sciences - the need to understand the social world; and
- the criminal behavioural discipline – the need to understand the motivations behind the abuse of personal information.

An interdisciplinary, or multi-method pluralistic approach is not a new suggestion, certainly sociotechnical theory advocates the importance of examining the interdependency between the social and technical elements within a system, ensuring that each are not optimised to the detriment of the other [Fox, 1995; Clegg, 2000]. Taking an interdisciplinary approach was highlighted by Hannay et al [2007] in a review of the use of theory in the software engineering discipline . Software engineering theories were

combined with cognitive psychology, social and behavioural sciences and information systems. Mingers [2001] advocates using a multi-method or strong pluralistic approach to address complex research situations. By making use of different research methods originating from different paradigms, or sets of general assumptions, perspectives of the reality of the situation can be explored from differing aspects, thus providing both a rich understanding and the possibility of triangulation.

Utilising qualitative methods has become an accepted part of the requirements engineering process [Sommerville, 2001; Nusibeh and Easterbrook, 2000], however, Ronkko [2002] suggests that the cross-disciplinary approach has difficulties because of the differences in interpretation between software engineers and social scientists. The context of understanding can be lost or misunderstood if qualitative data is interpreted using a quantitative framework. Also, the check-list approach favoured by software engineers does not allow for complexity within social phenomena [ibid].

4.2.1 Epistemology

The approach advocated by Gregor [2006] for the Information Systems discipline, makes a starting point to embrace a particular epistemological, or theory of knowledge, approach. For this research, and the leanings of this researcher, appropriate elements were found to be:

- Constructivist;
- Attention to the marginalised;
- Experiences of others;

- Action for change; and
- Ethics.

4.2.1.1 Constructivism

The constructivist approach focuses upon how humans transform and manipulate what they observe in order to make sense of it [Preece et al, 1994]. Meanings and understandings emerge from social encounters experienced by individuals, and any gaps in understanding are constructed from observations [Suchman, 1991]. Embedded within the constructivist approach are symbolic interaction and critical theory, both of which consider how individuals alter their behaviour as a result of the meanings they infer from their surroundings. Because ideas change and adapt as a result of interaction between individuals and their social context, and given that behaviour is affected by social norms [Bryman, 2004], social life cannot simply be observed, an interpretation of what is observed is required. A good understanding of the social world can only be gained by an examination of how individuals select and interpret events [May, 1993].

A contrast to constructivism is positivism, an approach rooted in the natural and physical sciences [Bryman, 2004] which considers human behaviour in terms of cause and effect. Positivism posits that the only knowledge worth capturing is that which can be verified by sensory experience [Jary and Jary, 1995], is experienced or objectively measured. Ideas, motives, feeling and emotions are all discounted because they cannot be measured. The positivist interpretation is that facts in the social world exist independently of the interpretation attributed by individuals, and objectivity is defined in terms of the

researcher's detachment from the social world [May, 1993]. However, this does not account for any interaction between theory and research, where each influences and informs the other.

4.2.1.2 Attention to the Marginalised

Attention to the marginalised is an approach found in Feminist Research Methodology, an approach suggested by Waller [2005]. This theory focuses on the areas of knowledge most relevant to feminine experience or womens' lives, the suggestion being that traditional epistemology has not paid enough attention to these areas [Jary and Jary, 1995].

Waller [2005] maintains that there are common characteristics to feminist research methodology which are:

- Attention to marginalised individuals in their social context. The attempt is to ensure that every voice is either heard or effectively represented;
- Explicit consideration given to ethics involved in the research;
- Rejection of strict objectivity. Given that the choice of research is a subjective and political choice, the argument is that no research can be objective. The choices of what is measured along with the words used for reporting are also subjective.
- The experiences of individuals, background and stories form a valuable and critical aid to understanding social interaction. Case studies in the design value and elicit the shades of understanding of a persons' experience.
- Orientation towards change in social institutions, structures and cultures.

- Data collection methods utilised primarily fell into three areas, surveys, semi-structured interviews and ethnography.

4.2.1.3 Experiences of others

What is evident here is the overlap with the principles behind Sociotechnical Theory. The experiences of others are deemed important with the "values and mindsets" principle as espoused by Clegg [2000]. Understanding the impact of ICT and considering the context of the individual have also been advocated by Coakes et al, [2000] and Mumford [2003].

4.2.1.4 Action for change

Action for change combines the move towards changing social intuitions, structures and cultures with action research. Action research was originally proposed by Lewin [1946] as a series of cycles forming planning, action and evaluation of the results of the action. The understanding gleaned by critical reflection of the effects of the action was used in the next iteration of the cycle.

There are many forms of action research, Bryman [2004] describes action research as an approach whereby the researcher and the participant work together to first diagnose the problem, then to develop a solution. Curry [2005] outlines three steps for action research where the participants are heavily involved throughout. For the purposes of this research, participant involvement occurred for identifying requirements and then for evaluation, after a proposed solution had been designed and implemented.

4.2.1.5 Ethics

Ethics are a set of moral principles and as Quinn [2005] describes it as being the

systematic analysis of the benefit, or otherwise, of a course of behaviour. Within social research, there has been a tension between the way in which information is obtained and the end purpose of the information [May 1993]. By selecting individuals for whom breaches to privacy pose serious risks, a strong ethical framework must be in place to ensure that no further harm is inflicted. The research design must incorporate throughout a thorough ethical consideration for the safety of the participant groups involved.

There is a criticism in the literature that ethical theories do not underpin the design of software [Garfinkel, 2000; Solove, 2003]. One example of this can be seen where Oppliger [2005] stated that ethical considerations for privacy protection were outside the scope of his research. The sociotechnical approach has strong ethical guidelines with guiding principles of improving quality of life, and facilitating the participation of individuals in decisions that affect them [Mumford, 2003]. Social risks and problems have been ignored, largely due to the strong culture within organisations of sticking to traditional approaches, and seeking to maintain the status quo. In the face of this, potential dangers arise when developers devote themselves to purely technical matters [Coakes et al, 2000].

Throughout this research, strong ethical guidelines remained in place, ensuring that at all times individuals were aware of what the research aims were and allowing them the opportunity to withdraw at any time. Part of the process of creating the research plan required that ethical approval was obtained from the University of Plymouth, School of Computing Ethics Committee. A copy of the documentation is included in the appendices.

4.2.2 Qualitative Methods

Situated within the framework of the encompassing epistemological approach are the research methods used.. Of the two primary paradigms that Cresswell [1994; 1998] suggests underpin human or social science research, that of qualitative and quantitative inquiry, the research methods belonging to the qualitative realm were considered to be the most relevant. The reasoning being that, taking note of Ashby's Law of Requisite Variety [1958] which states that a control system needs to be able to control the number of variables within a system, the number of variables that would be required to be observed could not be measured at an early stage and would best be uncovered through qualitative methods. Strategies of qualitative inquiry have been long established within the social science discipline, enabling researchers to study social and cultural phenomena [Myers and Avison, 2002]. Primarily, qualitative study is based on the process of understanding social or human aspects by building a complex, holistic picture, conducted in a natural setting. The populations chosen to participate in this research are likely to be comfortable with the qualitative approach, and the researcher is able to be situated in an active learning role, rather than as an expert passing judgement [Cresswell, 1998].

In contrast, the quantitative approach is based on testing a theory composed of variables that are measured with numbers with the analysis based on a statistical interpretation of those values. However, during the early stage of this research, applying values to variables was considered to eliminate important factors and potentially exclude important elements which may have relevance but are difficult to measure . Another problem arising with the quantitative approach is that statistical tests require a precise approach to measuring [Galliers and Land, 1987], which is not possible due to the subjective nature of

interpretation of risks. Mention should be made here of Likert scales [Likert, 1932]. These provide an interesting example of numerical values being attributed to something that is subjectively measured, which can then be subject to statistical interpretation. Likert scales were utilised in the evaluation stage as a means of capturing specific values for attitude and this is discussed further in section 9.3, the prototype evaluation.

Three research approaches selected from the strategies for qualitative inquiry were:

- Case Study;
- Phenomenology; and
- Grounded Theory.

4.2.2.1 Case study

Yin [2994] describes the case study as a form of observation best suited to exploring a contemporary phenomenon in-situ, thus being useful when the boundaries are not entirely clear. The technique can be utilised to examine and analyse in depth a single situation [Bryman, 2004] and is a suitable approach for those situations when seeking answers to *how* and *why* questions. Case studies draw from a selection of different methods for data collection and analysis strategies. The qualitative techniques of interviews and observations allow for the holistic and meaningful characteristics of the context to be recorded [Yin, 1994; Ghillham, 2000]. However, other quantitative methods may also be employed within the case study framework, should they be considered appropriate and useful [Bryman, 2004]. Clear aims and propositions in addition to the use of multiple

sources and clear chains of evidence are advocated, to ensure that the correct data has been collected, [Yin, 1994].

Selecting candidates from the appropriate population requires careful consideration, ensuring that carefully defined criteria, wholly appropriate to the research aims, are applied to the selection process [Yin, 1994]. Bryman [2004] describes how cases should be chosen not because they provide examples of any extremes or are unusual, but because they best suit the context of the research aim.

In this research, the case study approach influenced the way that data was collected. The data collection techniques sought explanations of the risks to marginalised individuals, to explore individuals' experiences and to incorporate an ethical approach to the data collection.

4.2.2.2 Phenomenology

Phenomenology is a descriptive study focusing on the way that humans experience their world [Jary and Jary, 1995]. The emphasis is on the meaning that individuals attach to their environment, rather than accepting that there is an externally applied social structure. Individuals build their own idea of a structure that is shared across society, usually termed "common sense" knowledge, which changes over time [Haralambos and Holborn, 1991]. Suchman [1991] considers that this knowledge is a problem focused social construction. Phenomenologists believe that it is impossible to measure human behaviour objectively, because humans create their own meanings through their interaction with others in

society, and so categories are created to aid understanding. Those categories are subjective and depend heavily upon the opinions and bias of the observer [Haralambos and Holborn, 1991]. Problems arise when the assumptions made about knowledge differ between individuals. The shared meanings are important for social interaction, and individuals need to share the same meaning [Bilton, 1987].

Using phenomenology to understand technological impact is not new, having been advocated by Boland[1985], and as illustrated by Introna [2005], the unifying feature of previous studies is the view taken that technology and society help build each other in a reciprocal and ongoing relationship. Ciborra [2006] argues that the phenomenological approach, whereby concern about concern is observed, be utilised in further work. Ciborra's work concentrated on the use of technology in the banking and insurance industry. Here, Information and Communications Technologies (ICT's) play a major role in the calculation and trading of risk, risk being considered in terms of actions, events and imagined outcomes and values. ICTs are important for storing data on accidents to calculate probability of risks, in addition to being the source of new, as yet, unmeasured risks. The benefit of the phenomenological approach, as perceived by Ciborra [Ibid], is that the intricacies of the situation can be collected and utilised. Jackson et al [2004] point to the importance of understanding the social meaning of a given hazard, and to building upon the previous work based upon public and expert perceptions of risk.

In terms of software design, phenomenology has been used as an important element in understanding how the design process has been affected, but is not yet commonplace and the literature is sparse. Bias is introduced into the design process by the individuals

involved because of the meanings that they attribute to things [Ohman Persson, 2004]. The nature of software engineering is such that the analysts and designers create software based on their own understandings. Boehm [2004] highlights the usefulness of the phenomenological approach in this situation. Phenomena have a rapid state of change, flow of data or software artefacts are not static, and therefore an approach which builds upon an understanding of the phenomena is required.

Understanding the phenomena of risks, as experienced by individuals, forms an integral element of this research. Demonstrating the constructivist approach, phenomenology combines with grounded theory to provide an explanation of the risks encountered.

4.2.2.3 Grounded theory

Grounded theory is the approach used to examine social processes that shape interaction allowing for emerging behavioural patterns within a group to be discovered. Software programs designed to analyse qualitative data have grounded theory as a central tenet. Concepts and categories emerge from the coding and refinement of data [Bryman, 2004]. Theories are generated from data from a specific area of study that is systematically gathered and analysed. The data represents the reality of the situation observed, offering insights for understanding leading to more meaningful further action [Strauss and Corbin, 1998]. Grounded theory overlaps with the phenomenological approach, the ways in which the data is categorised will be heavily influenced by the aims of the research and the theoretical interests of the researcher, thus adding subjectivity and bias [May, 1993].

Grounded theory has gained popularity with empirical studies using it in combination with

other conceptual frameworks. For example, Lee et al [2007] combined grounded theory with case studies to explore the social issues surrounding integrated information systems. Lee and Kim [2007] used grounded theory to analyse issues surrounding e-government initiatives. Winkleman et al [2005] found grounded theory useful to examine patient perceptions of technology within a health-care setting.

As originally outlined, Grounded Theory emphasised theory emerging from data without any predefined framework in place [Glaser and Strauss, 1967]. However, for this research, this was not an entirely appropriate fit. The framework influencing the data collection and analysis was that of consideration of risk and the participants understanding of that risk.

4.2.3 Risk assessment and situational crime prevention

Added to the combination of social theories and research methods are two paradigms that can be found within the criminal behaviour domain, that of risk assessment and situational crime prevention. These two approaches are used within the action for change element as noted above in section 4.2.1.4 and influence the design of the prototype.

Risk management is a complex area where the assessment of risk is highly subjective, relying upon experts in the field to determine where the risks lie. There is a danger that if simplistic techniques are used, strong assumptions are made that will be removed from the reality of the situation [Lefley, 1997], and so create some "knee-jerk" responses.

The previous chapter outlined how risk assessment is being incorporated into Privacy

Impact Assessment (PIA). PIA places risk as a central tenet of the whole design process, encouraging developers to examine how the data will flow in and around their systems. Risk as a central theme does, however, raise the question on how this will be assessed. Raab and Bennett [1998] propose that risk is best assessed through a combination of expert knowledge and objective calculation of risk, thus accounting for the subjective viewpoint. Subjectivity has its' place, it can serve as a pointer to areas that need further, more objective approaches, and works well when combined with other viewpoints to create a holistic perspective.

A classification of risks will help those carrying out a risk assessment and such a classification could best be created by utilising a taxonomy. A taxonomy is an organised structure that serves as a useful lens for classifying and understanding a body of knowledge [Carr et al, 1993]. Concepts can be logically ordered into groups and categories and so risk assessment can be carried out more effectively because of the way that the taxonomy aids the understanding.

Situational crime prevention (SCP) is not part of mainstream criminology because it places the focus on the relationship between the opportunity for crime to occur, the setting for the crime and taking measures to prevent the occurrence of the crime [Home Office, 2006]. Criminal activity is reduced because behaviour is channelled in such a way that opportunities for crime do not arise [Garland, 2000]. Originally 12 techniques to prevent street or predatory crime were proposed by Clark in 1993, but later in 2003 this was updated to incorporate 25 techniques falling into five specific categories viewed from the perspective of the offender [Clarke and Cornish, 2004]:

- Increase the effort – fit immobilisers in cars, or entry phones.
- Increase the risks – improve street lighting or use speed cameras;
- Reduce the rewards – remove car radios or gender neutral phone directories;
- Reduce provocations – efficient queuing systems, fixed taxi fares;
- Remove excuses – clear speed signs or litter bins in place.

However, SCP has fallen from favour in its own right and has now become subsumed into the realm of risk management [Clarke, 2000]. One of the criticisms is that the focus is upon the victim to take responsibility for their own actions [Felson and Clarke, 1997], the premise being that an individual should bear some of the responsibility for their actions should they choose to take a known risk.

4.3 Research design

This research design draws upon the methods introduced in section 4.2 in varying degrees. Assumptions and modes of thought influence how the research questions and aims are formulated, and how the methods are implemented. As discussed earlier, the combination of methods allows for an understanding to be made of the complexity of the personal privacy situation, whereas utilising one theory in particular would restrict that understanding. The research design provides the logic to link the data with the question and the conclusions, and as such requires that the unit of analysis be identified as personal information [Yin, 1994; Yin, 2003]. Personal information is considered to have a correlation with risk, the hypothesis being that the less personal information that is divulged, the less of a risk is posed.

Figure 5 offers an overview of how the underlying frameworks and theories fit together and underpin the research activities.

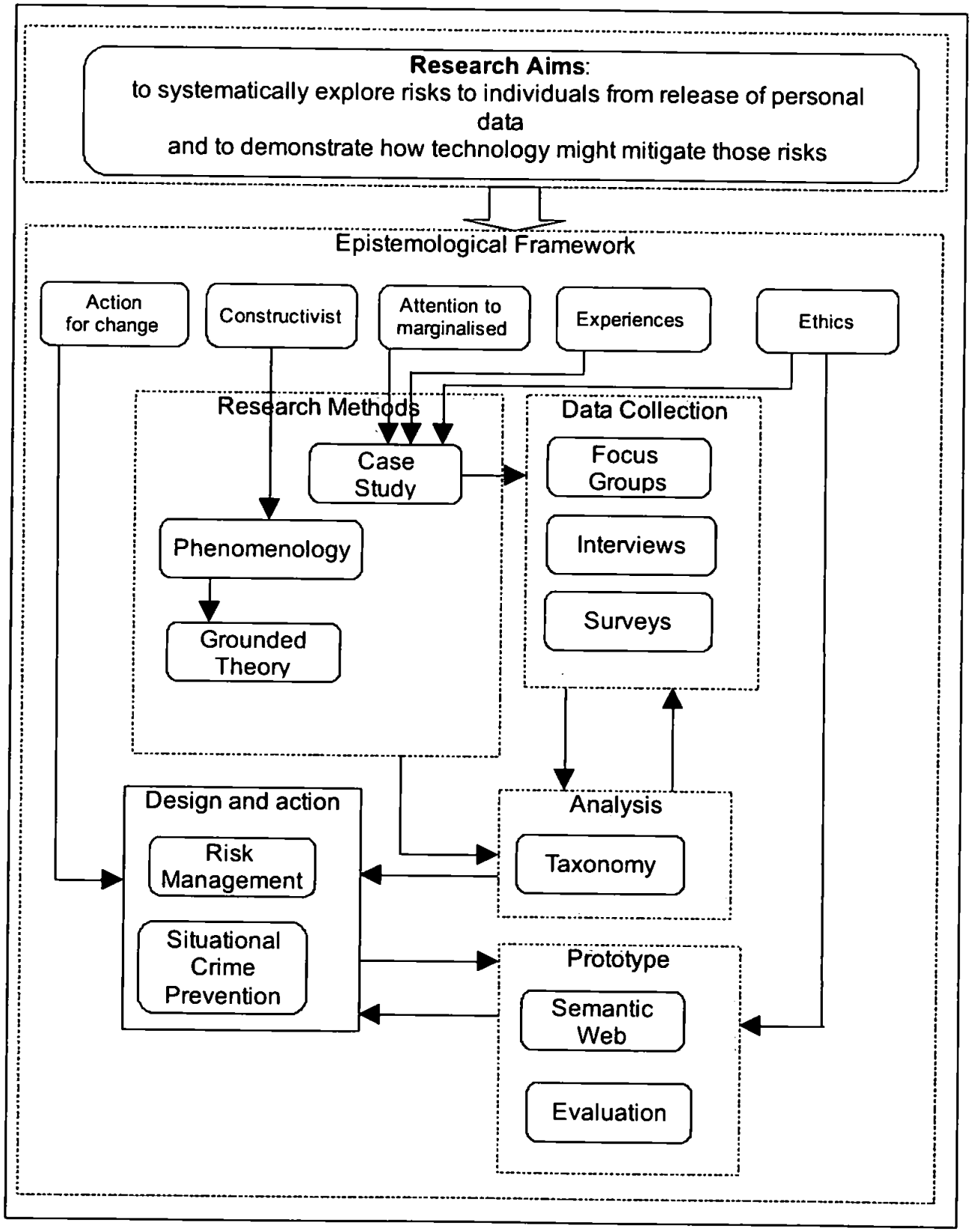


Figure 5: Research Space

The research space illustrated in Figure 5 above is characterised by the researcher's interaction with the literature and the formulation of the research aims and objectives. For the purposes of demonstrating the research space, these are summarised as follows:

- to systematically explore risks to individuals from release of personal data; and
- to demonstrate how technology might mitigate those risks.

The summarised research aims feed into the overall epistemological framework. This framework incorporates elements from both sociotechnical theory and the feminist research methodology (FRM) as expressed by Waller [2005], in combination with the constructivist approach. The relevant elements taken from the FRM are:

- Attention to the marginalised;
- Value of experiences;
- Action for change; and
- Ethical framework.

The constructivist approach of considering the constructs that individuals create to understand their social world is also an element within the framework. Within the epistemological framework are the qualitative research methods and the approaches adopted for design and action. The ethical frameworks are not just incorporated into the case study design, but also form a basis for the prototype. The case study design is influenced by the multiple elements of attention to the marginalised, and their experiences. The data collection approaches utilise the qualitative methods indicated, and are in turn

influenced by them.

Phenomenology and grounded theory demonstrate the constructivist approach. The analysis of the data collected creates the taxonomy, which not only is validated against the data, but is utilised by the design and action approaches. Risk management and situational crime prevention theories form part of the basis that informs the prototype development along with the findings from the taxonomy. As mentioned earlier, the creation of the prototype takes into account the ethical framework and demonstrates the Semantic Web design, implementation and evaluation. To complete the loop, the feedback from the prototype evaluation influences the risk management approaches utilised.

4.3.1 Selection of population

Raab [2003] made the observation that privacy risks had an unfair distribution, meaning that some groups of individuals suffer from more breaches of privacy than others. A measure of the distribution of privacy risks was not available, and so to explore fully the privacy context in which individuals found themselves, the populations for study were selected on grounds of propensity towards vulnerability. The concept of vulnerability and the link between the amount of personal information divulged and vulnerability has already been introduced in section 3.3 . In bringing vulnerability into the selection criteria for the target populations, a value judgement surrounding what constituted vulnerability had to be made. For the purposes of this research, vulnerability was therefore considered in terms of the effects of privacy breaches, and the populations needed to represent those who would potentially suffer the most serious risk of harm from any privacy breach. Two

groups emerged as having the potential to be considered the most vulnerable, domestic abuse Survivors and teenagers. No other groups of individuals were considered as likely candidates as these two groups were accessible by the researcher and appeared to fit the required vulnerability profile as suggested by Raab and Bennet (1998)

Victims of domestic abuse, hereafter referred to as Survivors, endure many episodes of violence before seeking help [Yearnshire, 1997], but the time they are at their most vulnerable is when a decision to leave an abusive relationship and seek refuge is made [WAFE, 2002]. At this time, control over personal information is very important. As a distinct group of individuals, they are most likely to experience *"dataveillance"* [Clarke, 1999] technologies being used against them.

Teenagers are considered to be most at risk of stalking and predatory sexual attack [Magid, 2004]. These young people increasingly explore the boundaries of the technology that surrounds them, and often in ways that their parents do not understand. They embrace the social nature of the Internet with many of them becoming adept at creating, manipulating and uploading content [Lenhart and Maddern, 2005]. Different web applications are utilised as a method of keeping up with the peer group and the consequences of actions are not always considered. Vulnerability for this group is not a concept that they themselves would necessarily admit.

4.4 Reflection on methods

Emerging from the research space were issues of exploring and understanding the complexity inherent within. Having considered all the available and relevant approaches to

research, it became evident to the researcher that a best fit would be created by utilising a selection of methods from a range of disciplines, illustrated by Figure 6. Each discipline brought with it methods and theories to explain and explore, yet each when viewed alone

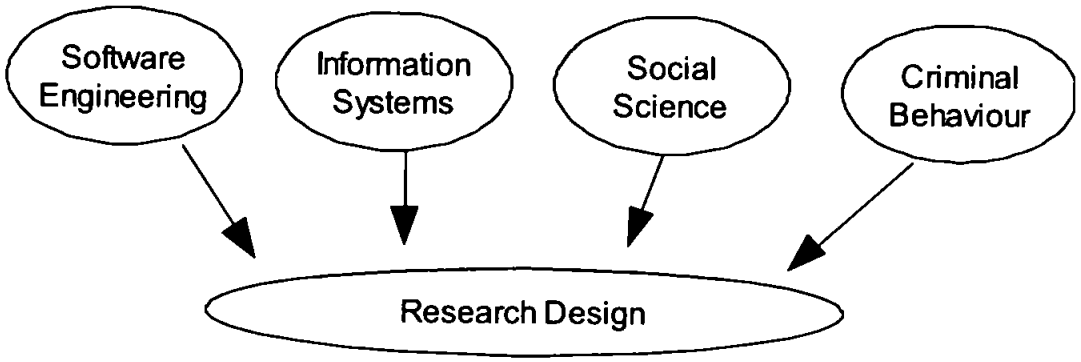


Figure 6: Cross Disciplinary Areas

had failings and was not quite the best fit. Whilst Mingers [2003] proposes this multi-disciplinary approach, this specific combination of approaches currently has no literature available to describe it.

Utilising social theories of interpretations in the research design raised issues of subjectivity. Meanings attributed to words, and the design of the questions were heavily influenced by the researcher's frame of mind, which would appear to confirm the argument proposed by May [1993] that it is difficult to neutrally observe the social world. Assumptions and stereotypes held by the researcher, and society, are not explicitly highlighted and are hidden and therefore perpetuated. There is a requirement that the research design be cognisant of the assumptions and limitations posed by the researcher. There is not a strict separation between fact and values because values are a fundamental part of being human, and that in turn will affect the judgements made about how the research is carried out. Encouraging situations of disengagement, where the researcher

does not over-identify with the research, does not allow for any retrospection on dialogue or open exchange between researcher and participant. This is seen by May [Ibid] as devaluing the personal experience, and does not account for the many ways in which the researcher will be affected by the research undertaken. It is because of this reasoning that the researcher chose to identify with some of the elements taken from Waller's [2005] analysis of feminist research methodology.

Quality of research design is most often demonstrated through ensuring that there is reliability, validity and relevance [Bryman, 2004]. Reliability concerns itself with the issues of consistency of the measures and is demonstrated through reliable management of the data collected. Reliable management is demonstrated in this research through the use of effective data management controls, utilising software analysis programs such as QSR N6[1] for coding, and Microsoft's Excel[2] package for storage of tabulated data. Validity concentrates on ensuring the integrity of the conclusions and is tied in with reliability. There are different approaches to validity, however only external validity is really applicable in this situation, because this research does not attempt to provide a generalisable theory. External validity here is demonstrated in the case study approaches, by ensuring that there are multiple sources for data so that triangulation can be carried out. The cases themselves were chosen because they were best suited to the context- privacy was an important issue, not something that would easily be dismissed. The evaluation of the prototype was carried out by the selected population to demonstrate validity in the design. Relevance considers the importance of the topic or the contribution to the field

[1] www.sqrinternational.com/products.aspx
[2] www.microsoft.com

[Bryman, 2004].

4.5 Conclusion

The differences between the relevant disciplines were considered, prior to the description of the many different research approaches utilised to underpin the research design. The suitability of the methods for exploring the social world determined which were utilised and which were most appropriate for this research.

The research design illustrated how the different methods fitted together into an intellectual framework, built the plan of action and addressed the need for appropriateness. The encompassing epistemological approaches, built from constructivist, sociotechnical and feminist research methodology, fit into the research methodsdiscipline. These approaches allow for the assumptions and modes of thought that bias the creation of the research questions, aims and methods of collection and analysis.

The novel, cross-disciplinary approach adopted encompassed the combination of epistemological approaches from the social discipline, the explanation theories from the information discipline, situational crime prevention from the criminal behavioural discipline with all elements being melded together to create a relevant research design to address the requirements. The research approach was to collect information from carefully selected populations, exploring their thoughts and feelings through discussions and focus groups. The concepts articulated by the respondents, as understood by the researcher, were formulated into a taxonomy to aid understanding and, further, into creating the requirements for a prototype piece of web software.

The chapters that follow articulate how these methods were implemented and the resultant findings.

5 Determination of Risks

This chapter outlines how the research design introduced in chapter 4 is implemented. The implementation and findings for each of the populations investigated are introduced in turn, followed by an explanation of the validation exercises. The chapter concludes with the results of coding the data collected.

5.1 Introduction

The first phase of the research was to systematically explore the risks arising for individuals. This was achieved by gathering information about risks faced by the selected populations, utilising the case study approach as discussed in section 4.2.2.1 . The data collected was validated against a messenger survey and verification of online presence prior to being evaluated. Evaluation was conducted using the techniques expressed in sections 4.2.2.2 and 4.2.2.3 of phenomenology and grounded theory to create categories of data to aid understanding.

5.2 Implementation

Implementation of the research design took place examining three target populations;

- Individuals who were not IT professionals.
- Domestic abuse survivors
- Teenagers.

The opinions from individuals were collected through semi-structured interviews. Interactions with members of statutory and voluntary sector bodies in the field of domestic abuse were conducted through semi-structured interviews and workshops. Focus groups

were carried out where young people could discuss their views on personal privacy and interaction with the Internet.

5.2.1 Individuals who were not IT professionals

The first step for the implementation was a small experiment and online survey designed to test out questions and to develop realistic scenarios for use within the discussions with teenagers. The objectives of the experiment were:

1. to determine how people perceived the world wide web in terms of feelings of vulnerability and/or intrusion into personal privacy.
2. to ascertain the extent to which the Internet divulges personal information.

Ten respondents were selected through personal contacts and referrals from two of the initial contacts. The initial contacts were originally selected because they were not software or IT professionals, they did not view themselves as technology experts and they fitted into the demographic categorisation illustrated below.

The respondents backgrounds were classified according to the Office of National Statistics socio-economic classification system [ONS, 2002] illustrated in Table 1. Whilst an effort was made to ensure that there was a good cross section from all the social grades, it has to be acknowledged that this is not the most suitable method for sampling a population as it can introduce bias. However, this did appear to be the most appropriate available method for sampling a very wide, and potentially hard to access population.

Grade	*Status*	*Occupation*
I	Professional	Higher managerial, administrative or professional.
II	Managerial and technical	Intermediate managerial, administrative or professional
III N	Skilled occupations – non-manual	Supervisory or clerical, junior managerial, administrative or professional.
III M	Skilled occupations – manual	Skilled manual workers
IV	Partly skilled	Semi and unskilled manual workers
V	Unskilled / unemployed	State pensioners, unemployed, casual or lowest grade workers.

Table 1: Classification Description

The experiment took part in three stages:

1. A semi-structured interview was held with the respondent where questions were asked to determine their current level of knowledge. A copy of the questions asked are included in Appendix A – Questionnaires.
2. A search was made for publicly available information that was accessible through the Internet.
3. A second interview discussed the findings and asked for the respondents opinion on the findings.

The first stage involved a tape recorded semi-structured interview. This followed a full explanation about the nature of the experiment and obtaining consent from the respondent for the searches. The semi-structured interview allowed for flexibility within the framework of the interview, allowing the researcher to explore issues with the respondent as they arose. The respondent was asked in this initial interview about their perceptions of the

Internet in terms of divulging personal information, and their ideas about the risk posed to themselves. This was also the opportunity to explore any concerns they had about information available.

The second stage was to conduct a search through the Internet to discover publicly available information using the search terms of the respondents name and their address. Only in some of the cases did the researcher have prior knowledge of their date of birth. The search was not designed to be exhaustive, but to demonstrate how much information could be discovered over a short time period and for a small financial cost. The websites chosen were those which provided personal data to the general public. The experiment used a combination of eight standard search engines, electoral roll websites, and public record websites. Search engines were queried for standard web pages, images, discussion board entries, blog entries and news entries. The UK public record websites included the General Register Office and Land Registry, which are described below. Social networking websites such as Friends Reunited were also used. Searching was limited to the first five pages of the search engine results, as research has found that searchers tend to disregard pages beyond page five as irrelevant [Ding and Buyya, 2004]. All results were recorded along with the time and total cost of obtaining the information. Whilst Google was considered the most popular search engine, according to Neilsen NetRatings in 2006 [Sullivan, 2006], other search engines were selected for comparison. A table of the websites along with brief details is given below in Table 2.

Website	***Description***
www.google.co.uk	Search engine.
www.yahoo.co.uk	Search engine.

Website	*Description*
www.altavista.co.uk	Search engine.
www.askjeeves.co.uk	Search engine.
www.dogpile.co.uk	Search engine.
www.excite.co.uk	Search engine.
www.search.com	Search engine.
http://blogsearch.google.com	This beta version started indexing blog sites in 2005 and specifically targets blog entries for indexing.
www.192.com	UK focused and provides historical electoral roll details, public current electoral roll, directory enquiries, business directory and director reports.
www.upmystreet.com	Portal for discovering information based on a postcode. Links displayed to local businesses based on postcode. Property prices for properties sold in the locality are shown from data collected from land registry.
www.companieshouse.gov.uk	Companies House is a government department, the website provides access to information held on all UK companies. Offers searches for companies and company directors.
www.peopletrace.com	Service offered to general public for tracing individuals. Online database offered with details collected from the public electoral roll.
www.electoralrolluk.co.uk	At the time of the study carried out, this offered information gleaned from the UK electoral roll. At the time of writing, 2007, the service had closed.
www.bt.com	UK telecommunication service offering a search facility for those who choose to appear in the telephone directory.
www.mobilephonenumber.com	Offering searches for mobile phone numbers for UK, Canada and USA. Reverse look up searches also offered.
http://mobile118.co.uk	UK Mobile phone directory.
www.multimap.co.uk	Mapping service allowing searching on postcodes and aerial photographs.
www.friendsreunited.co.uk	Website allowing people to link to schools, workplaces and addresses.
www.genesreunited.co.uk	Genealogy website allowing people to build family history and interact with others.

Website	*Description*
www.missingyou.net	At the time of the study this allowed searching for individuals. Names could be registered with the website. At the time of writing this is not available.
www.landregistry.gov.uk	Government website allowing access to the register of title to land in England and Wales. Electronic copies of title deeds available for download for a small fee.
www.hmcourts-service.gov.uk	At the time of the study this was based with the UK Home Office. At the time of writing is now an executive agency of the Ministry of Justice. Their remit is to manage the courts of England. This website gives searchable information about crown court cases and judgements.
www.bailii.org	Offers searching on British and Irish case law and legislation.
www.insolvency.gov.uk	Provides access to the Individual Insolvency register. This contains details of bankruptcies that are current or have ended in the last three months; current and individual voluntary arrangements and current bankruptcy restrictions orders and undertakings.
www.1837online.com	At the time of the study this was launched by the general record index to meet the demand for online genealogy studies. Originally, only details of the general record office indexes were given. With this information individuals were able to purchase the full certificate from the General Record Office. This has since been relaunched as www.findmypast.com offering a far more comprehensive family history service.

Table 2: Websites used in searches

From the searches a report was created detailing the sites accessed and the exact findings. A conclusion was written considering the implications of the findings and suggesting methods of addressing the issues that arose. This report was presented to the individual and, after allowing a period of time for the individual to read and consider the report, a second, recorded, semi-structured interview was held. The conclusion was not attached to the report but was released to them after the interview so that their responses

were not influenced by it. The respondents were invited to discuss the nature of the information discovered and to explore their feelings about it. The questions posed to start the interview are included in Appendix A – Questionnaires.

5.2.1.1 Individuals - Findings

During the initial interviews, five out of the ten individuals were uncertain as to the amount of information that could potentially be available. Two respondents attempted a guess at the amount, with one suggesting that whilst there might not be very much, what would be available would be linked to credit.

> *"I really have no idea. I wouldn't imagine that much, but then of course if it's things like credit card numbers and details and credit worthiness and all those sort of things....".*

And another respondent suggesting that bank account details might be gleaned.

> *"I don't really have much of an idea at all really. I would imagine you could probably find out my full name, date of birth, possibly what bank account I've got..".*

One male from the professional category had a very clear idea of what was available and included within his list secondary use by companies selling on his information. One female within the unskilled category articulated her extreme anxiety about information held, believing that there was a large amount.

The findings from the searching activity discovered that the date of birth was key to obtaining identity documents. One of the respondents was found to have their date of birth publicly available over the Internet. In this instance the full General Records Index birth entry was listed on a web page created by a member of the Guild for One Name studies. The Guild is an organisation for individuals researching all occurrences of a specific surname. The date of birth was found to be vital to finding out more public information, for

example mothers maiden name, and provided access to purchasing full certificates.

For one respondent, further information was gleaned about the family from the Friends Reunited website. From here the date of marriage and birth details of the children were able to be found. Primary and secondary schools for the respondent were also listed, which had implications for the security questions asked by the online banking service for this respondent.

The current electoral roll provided information on only two of the respondents. For one respondent, the website 192 combined the information from a directors report with public electoral roll information. The respondent, a director of a company, had been very careful not to divulge the private home telephone number, however, this number was listed with the partners electoral roll details. Nine of the ten respondents had chosen to be ex-directory with the tenth respondent ensuring that no gender specific information was displayed.

Two respondents had popular names with one sharing their name with a famous actor. This gave a level of anonymity, it was difficult to be certain that the information found pertained to the respondent. Further corroborative information was required to find exact matches.

During the discussions with the respondents it became evident that access to mother's maiden name through the General Records Index caused concern.

"...the biggest concern is the fact that banks and credit card companies use mother's maiden name

as a reference point.....the fact that somebody has listed my mother's maiden name without my consent, given that it is used so much as a reference for bank details etc.....".

This prompted one respondent to contact their bank and change their identity details. Financial interactions were of concern to four of the ten respondents, who were concerned about the possibility of Identity Theft. One respondent felt that any computer system was unsafe and was in jeopardy of being hacked into to obtain financial information of customers.

"I can't believe that anybody's system is hack proof, nor any banking information either".

Three of the respondents stated that they would not use Internet banking because of the fear of details being prey to fraudulent use, one of those three stated that they would not use credit cards for that same reason. Two other respondents exercised caution in their financial dealings online, always looking for the secure website to enter credit card details when making purchases, ensuring that purchases were made from reputable companies with a web presence, with one respondent being careful about the purchases they made. Credit references and the use of credit cards were cited as one area of concern for three respondents. Information divulged was felt to be pertinent to credit profiling and listing by credit reference agencies, as well as linked to the use of credit cards.

"..if, perhaps, I was to apply for, say credit of some sort, there might be erroneous information on the net which might stop me from getting that, or things of that kind.".

Two of the respondents linked the Internet with surveillance activities, relating it to the Orwellian concept of "big brother". One male, category V respondent, believed that there was too much observation conducted through the Internet, and one female class IV expressed her concern at the intrusive society. In contrast, one male category II

respondent believed that there were too many people for observation through the Internet to be effective, and one category V female respondent believed that she was not of interest to other people.

Three respondents believed that the amount of information available about them would be directly in proportion to their interaction with the Internet, and because of this, one respondent felt it important not to have any interaction with the Internet at all. Two respondents perceived that the Internet facilitated fraudulent behaviour. One respondent stated they would be wary but confident of not being taken in, in the same way that they would approach telephone calls.

> "*I think I'm fairly compes mentis to not be taken in by fraudsters, like over the telephone, as the same as over the Internet.*".

Four out of the ten respondents expressed surprise about the publicly accessible information, with two voicing concern about it. Two single female respondents considered there to be a risk from the divulging of their address, making the point that it was possible to calculate that they lived alone from their land registry details.

> "*I don't particularly like this Land Registry thing which gives me as the registered owner of the house.... I don't know that a woman living alone wants to be seen as the owner of a property, because normally as an owner of a property it would be Mr and Mrs so and so. So one assumes that automatically people then know that I'm living alone.*".

This made them feel very vulnerable, with one being concerned about being attacked or burgled and the other concerned about malicious telephone calls, based on previous experience.

"I would perhaps feel more vulnerable of being burgled or something like that, or possibly being attacked for example".

However, a male respondents view was that although he was surprised that the land registry details could be accessed, he did not feel there were any information divulged that caused concern.

5.2.2 Survivors

This second population were selected for their representation of a potentially vulnerable group, the discussion regarding how and why this population was selected is to be found in section 4.3.1 . For these individuals, there is a potentially greater risk from privacy breaches, the effects of the breaches have the potential to cause further harm and suffering and are a likely group to face more privacy risks than others. Survivors are monitored carefully by the perpetrators of abuse due to the nature of the behavioural traits centring around issues of power and control. It was therefore very important to ensure that the influence of the research and the researcher did not place any Survivor in a dangerous situation. Ethical responsibility became of utmost importance at this stage. The ethical approach required that the researcher must protect participants from physical and psychological harm at all times during the research. Because the influence of the researcher was likely to impact a Survivor's life, either through discussions or contact, it was viewed that this would put the Survivor at risk. The safest approach for the Survivor was, therefore, to explore their privacy issues vicariously. Therefore, front-line staff were selected, as they could give a broad overall perspective as a result of their familiarity with the target population, their broad experience of different situations encountered during the course of their work and would be less likely to be under intense duress and frightened about what might happen to them.

Semi-structured interviews were held with three managers of refuges, two outreach workers and one probation officer involved with delivering cognitive behavioural programmes for perpetrators. In the initial discussions the respondents were asked to categorise different technologies in terms of levels of threat, choosing between a measure of high, medium or low. The questions posed are provided in appendix A Email correspondence took place with an officer based within the Plymouth domestic abuse unit.

In addition, a couple of two hour conference workshops were held at the Women's Aid National Conference in 2006 involving 15 participants each. The participants of the workshops were workers from both refuges and outreach services, all working with domestic abuse survivors. The workshops were aimed at exploring the uses and abuses of technology. After the introductions, an outline was given of the workshop followed by splitting the group into two with each separate group discussing either the advantages or disadvantages of technology. These were fed back to the group as a whole with discussions generated from the findings. Only one of the workshops had time to present a discussion on the current influences of technology and a discussion of the issues arising. The findings presented in this research are those from the discussions held prior to the presentation.

5.2.2.1 Survivors - Findings

Concerns were raised about the potential risks and ease with which a flow of personal information could be divulged through mobile phones, emails, social networking websites, personal websites, public records and third party databases. The categorisation exercise

gave an indication as to which technologies were perceived by the respondents to carry the most risk. In order to place these technologies into an order, the following values were attributed to the responses: Low = 1, Medium = 2 and High = 3. This did highlight that whilst instant messaging and the Internet were described in the interviews as quite high in terms of the effect of the risk they carried, because Survivors had little opportunity to access these facilities, the chance of occurrence was quite low. This is reflected in the low culumulative score that these technologies were awarded. At the other end of the scale, however, mobile phones, email and third party data and the divulging of it was considered to be far more of a risk. The technologies are presented in ascending order below in Table 3.

Category	***Overall Risk Rating***
Instant Messaging	4
Internet	4
Personal Digital Assistants (PDA)	4
Prize Draws	5
Global Positioning Systems (GPS)	5
Radio Frequency Tags (RFID)	5
Digital Cameras	7
Loyalty cards	7
Cordless phones	8
Public Records	9
Mobile phones	9
External company databases	9
Email	9
Credit Cards	9

Table 3: Overall Risk Categorisation

It was acknowledged that whilst mobile phones provided an important role, at the same time they allowed information about a Survivor's whereabouts to be divulged and did cause issues for one refuge manager.

> *"In terms of the refuge mobile phones are a huge huge problem. ...if women fled they could get away from their partners without their partner knowing where they were, or hopefully not knowing where they were. Often the fact that women come with mobile phones and partners have access those numbers, means that there's all sort of different issues about what women can do about the fact that he's got, you know, you can have, ...quite often, where a woman is in the refuge and they talk to their partners, you know they are talking to them, which just seems a bit of an irony, you know, in that they are in a refuge to get away from them in the first place, you know where he has attacked them and the police have come to get them, and they are actually talking to them. "*

Two of the refuges discouraged their residents from using mobile phones, working with network providers to replace the SIM cards within the mobiles or to change the mobile phone numbers. For those women who were resettled the advent of location tracking services caused a concern, especially as mobile phones were found to be the commonest gift given to a child still in contact with the perpetrator. In following up the concerns raised by the respondents, the following question was posed to four mobile phone network providers in December 2005, Orange, T-Mobile, O2 and Vodafone.

> *"If a mobile phone was given to a child for a present, and that phone had a location tracking service set up on it, without the knowledge of that child, could the network provider tell the user of the phone if there was such a service, and who was providing that service, so that it could be stopped?"*

None of these network providers could inform a service user if there was a location forwarding service set up on their mobile phone number. The only indication was to be a text reminder issued from the location service provider to remind the owner of the handset that their phone was being tracked. The potential wait for this reminder text was between

14 to 30 days.

One outreach worker reported formulating careful plans for communication with their clients having identified using mobile phones for communication as a high risk. The high risk arose from the tendency of the perpetrators to monitor calls made and received through the call listings, viewing text messages received and listening to voice mail. Controlling behaviour using text and photo messaging was described by one respondent, who observed that since cameras had become embedded within mobile phones, perpetrators were insisting that photo messages be sent to prove where the Survivor was situated.

Increasingly, access to computers for residents in refuges was felt to be essential support tools. Reasons behind providing computing support fell into two categories. One was as a tool for children to carry out their homework and coursework. The other category was to ensure that residents were not disadvantaged in their interactions with housing authorities, local authorities and social services. Many housing authorities were conducting the application process for housing online. However, within the situation of a refuge, two problems were highlighted, one was that where personal information had been freely divulged not just about the residents themselves, but of other residents within the community of the refuge. The second issue was inappropriate access to gambling, pornography and online dating websites. All the respondents connected with the running of refuges were fully aware of the importance of ensuring appropriate access and data protection of personal information files held on Survivors.

Email communications and Internet usages were also viewed in terms of posing risks. Perpetrators were described as accessing email correspondence to determine whether the Survivor had access to support or visited support sites.

Public records were a well known problem among participants. One respondent reported that survivors were advised not to enrol on the electoral register, even though the electoral roll allowed individuals to opt out of having their address publicised. The reasoning being that address information could still be obtained by visiting the local government offices. However, at the time of writing there is new legislation coming into force which will allow Survivors the opportunity to register for the vote, yet keep their address secret (MOJ, 2007).

Public records not normally available to the general public, but which are mandatory and are sold on, created a situation where a Survivor was tracked through association. One situation was described where a support worker was traced to the refuge they worked for by the perpetrator accessing the UK Drivers Vehicle Licence Authority (DVLA) database. Measures had been taken to hide the location of the refuge from the perpetrator and the Survivor felt some measure of protection through that anonymity. The support worker had been mentioned to the perpetrator by name during various communications and this name was used to search the DVLA database accessed at work to discover the drivers licence and car details. The occasion was described as a chilling moment when the perpetrator called the Survivor on the mobile phone, informed her of the number plate of the Support worker's car, described its exact location in the car park of the Refuge and gave the Support worker's full name and address.

Tracking of refuges through postcodes was acknowledged to be made easier with the advent of Google Earth, multimap.co.uk, aerial photographs, upmystreet.com and 192.com. Some people made use of Royal Mail PO Boxes to hide real addresses and were not aware that the Royal Mail allocates postcodes for PO Box addresses according to the address of the property, not the nearest post office.

Information sharing between agencies working with affected families was raised as a concern, in the context of the ease of sharing personal information, facilitated by modern technology. Women's Aid have highlighted in a previous report [Saunders and Barron, 2003], the need for safeguards to ensure that details of a family are not used by perpetrators to track them down. The danger was illustrated when a standard report from a database was electronically transmitted to the perpetrator giving full details of the family concerned. 46% of respondents knew cases where contact procedures had been used to track down a partner. One respondent discussed a situation where the Children and Family Court Advisory and Support Service (CAFCASS) divulged the full name and address of a court case, leading to kidnapping of the child.

> *"What the CAFCASS officer did was to send copies of her report, and she sent her report along with her full name and address, so he knew her new name and her new address. He actually kidnapped the boy, ... it took the mother a year to get the boy back. Now she'd done everything right, again, that's paperwork, it might be computer generated."*

Other third party organisations were cited as causing a problem with divulging information. Banks were cited as an issue whereby it was becoming increasingly difficult for Survivors

to open new bank accounts, especially when temporarily situated within a refuge. Benefits now being paid into bank or building society accounts, rather than collected through benefit books, meant joint accounts were the only access for funds. Survivors were finding it difficult to move these payments into accounts held solely by themselves, and so were having to use joint accounts. One situation arose where the perpetrator was able to discover from the bank the exact cash machine that a Survivor routinely used, even though the Survivor had been rehoused in a refuge a great distance away.

> *"she went to use it [the cash machine] one day, and he was behind her. He'd questioned it, he'd ring up and say, there's a lot of withdrawals from this one in Plymouth, which cash point is it, I don't recognise it. The bank told him. He was waiting, he'd waited there for about a week."*

Other third party organisations cited as divulging personal information were:

- National Insurance – Survivors being traced through National Insurance numbers.
- Health Records – GP's divulging information.
- Utility company's – divulging new addresses for Survivors.
- Child Support Agency – divulging new addresses for Survivors.

5.2.3 Teenagers

The third population examined involved gathering the views of young people, aged between ten and nineteen inclusively. The reasons behind choosing this population are discussed in section 4.6.2. Teenagers represent a group of individuals who are exploring their world, making full and good use of the technologies available to them, however, they represent a potentially vulnerable group with regard to privacy risks and yet would appear to have different approaches to privacy concerns, perhaps, than older individuals. For

these reasons they were considered a useful group to examine.

Focus groups were considered to be the most appropriate method for gathering information from the teenagers. It was considered less intimidating for the teenagers to be able to discuss privacy issues as a group with the researcher, rather than be singled out for a one to one interview. Focus groups are used within the feminist methodology (as mentioned in section 4.2.1) as a way of addressing the potential for there to be a power imbalance between the participants and the researcher [Bryman, 2004]. Participants within the focus group are able to have more control over directing the discussions. In addition, one individuals thoughts can prove a starting point for another, leading to articulation of different avenues of thought that might not emerge if there were only two people conversing. There were also child protection issues to be considered within the ethical framework, good practice within any environment involving young people is that an adult should not be on a one to one basis with a child. There were disadvantages to be faced when using the focus group format, the need to ensure that discussions would be relevant without exerting restrictive controls, the need to ensure that people who wished to contribute could and also balancing the concern of others who might not wish to articulate unpopular concepts to the group.

Three of the focus groups were held with community groups and four were held in a school setting. Two of these seven were held with year twelve teenagers, one with year ten and another with year eight. Four more school based focus group transcripts were made available from the Trustguide [Lacohee et al, 2006] project which utilised the approach defined in this research. In total, one hundred and five young people were interviewed.

Prior to conducting the discussions, the young people within each focus group were issued with a questionnaire designed to elicit some broad demographic data around their Internet usage and to set the context for the discussions. The pre-group questionnaire was designed to focus discussions by encouraging the respondents into thinking about the topic matter, before the discussions about the scenarios began. To address one of the potential disadvantages of focus groups, the possibility that discussions do not address the issues being researched, it was important to set the scene and make the participants aware of the general topic area. In addition demographic information and Internet usage was collected. A copy of the questionnaire is in Appendix A – Questionnaires. In addition to the pre-group questionnaire a group word-storm approach was utilised where young people were asked to consider two topics. The first posed the question, how did personal information get onto the Internet and the second was to ask who saw that information.

The discussions were generated by describing a set of scenarios based upon an understanding of the problem situation, and encouraging the respondents to discuss their views, thoughts and feelings. The discussions were recorded onto tape for later transcription and analysis using QSR N6 software. The concepts extracted from the data were refined and structured into the taxonomy that is presented in the section 5.4 below. The findings from the first investigation, involving individuals, influenced the design of the scenarios and the questions posed within the focus groups and interviews. This demonstrates the grounded theory approach, whereby data immediately begins to influence the design of the research.

5.2.3.1 Teenagers - Findings

Presented below are the findings from the focus group questionnaires and represent an interesting snapshot in time, that of mid 2006. The participants within the focus groups represented a young age range being sampled, with the average age being fourteen years old and a range between eleven and eighteen. The genders were fairly evenly balanced with 45% female respondents, 55% male respondents. Of those young people, 83% used Instant messenger and communicated with friends using the Internet, with an even gender balance. Use of online diaries or "blogs", was not that high at 23%, with more female respondents than male respondents making use of blogs. My Space and Bebo were listed as the most common social networking websites. 64% signed up to websites that collected personal information, and 27% of young people were concerned about the information they had divulged.

The findings of the categories of Internet usage are presented in Figure 7, illustrating the gender breakdown. These findings are discussed below.

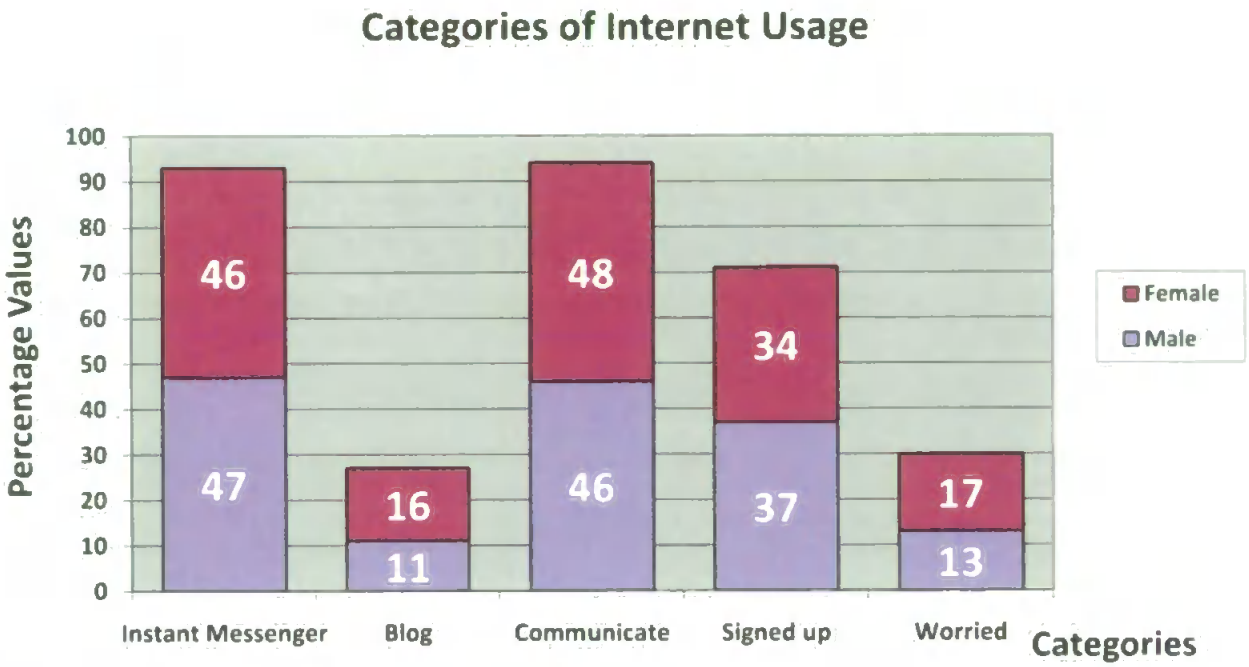


Figure 7: Focus Group Categories of Internet Usage. 2006

Fourteen categories of Internet usage emerged from the findings. A count was made of the number of times a word occurred in the answer, and is presented as a percentage in Table 4.

Category	*Percentage*
Research (Homework, Revision, Wikipedia, Work. Look things up, School, Coursework, information)	65%
Instant Messenger (MSN, Talking to friends, Chat)	41%
Games (Fun, online games, downloadable games)	30%
Downloads (Music, Videos, Pictures)	21%
Email (emailing friends, family and businesses)	16%
Shopping (e-commerce, ordering products)	9%
Visit Websites (Runscape, angrykid.com, football, News, children's websites)	6%
Social Networks (My Space, Bebo, Forums)	5%
General Surfing (Browse, Whatever)	4%
Internet Banking	2%
Events	2%
Meeting new people	1%
Finding Concerts	1%
News	1%

Table 4: Internet Usage

Although nine of the twelve focus groups conducted were held within school settings, the occurrences of the top category for "Research" were fairly evenly distributed amongst those groups and the three held in more relaxed settings. This category encompassed homework, revision, referencing wikipedia, looking things up for work, school work, coursework and information. The categories that followed illustrated more social uses, interacting with friends, playing games, downloading music or videos. Only one person described utilising the Internet to make new friends.

Whilst a lot of the young people made use of instant messaging, 23% made use of a blog or online diary. There were a number of young people who questioned the term "blog", to

which they were given the response "a form of online diary", suggesting that blogs were not as prevalent as the literature might suggest. The social networks also did not appear to be quite as prevalent, with 13% making use of social networks. The most common choice for online interaction was MSN Space with Bebo and My Space following in that order. It should be noted with these statistics that this is such a rapidly changing field. These measures illustrate usage in the middle of 2006, and no doubt social networks and blogs will be subject to the change over time.

The websites that young people gave personal information to ranged in type with the communication websites, such as MSN Hotmail or Google Gmail being the most popular. Other websites were hobbyist or gaming sites such as battleon.com, drwhobattlesinitiative.co.uk, fanfiction or justpaintball.co.uk. Shopping websites also featured such as ebay and Amazon along with freecycle. Websites for future careers also were remembered for collecting personal information, such as UCAS, Connexions and RAF Careers. The websites listed illustrated a wide variety of sites accessed.

In answer to the question concerning being worried about giving out personal information, only 27% of young people indicated their concern. The gender split was recorded at 16% of girls were concerned, 11% of boys. The small sample size means that generalisations cannot be made, but it would be worth further investigation to consider whether girls are concerned more than boys, as might be illustrated here.

From the word-storm, the answers arising from the first question, *how did personal information get onto the Internet*, illustrated a wide understanding of how personal

information was delivered to the Internet. These fell broadly into three categories, activities where individuals were personally responsible, third party posting and technologically mediated divulging. Personal divulging of data was seen when registering with websites, forums, mailing lists and for music downloads and interaction with games. Third party divulging of personal information was seen to occur with criminal records, commercial enterprises selling on data, identity fraud and school divulging. For technologically mediated divulgence, bluetooth and virus activities were seen to be threats. The responses to the second question, *who saw that information*, were almost unanimous across the focus groups, all the young people acknowledged that personal data posted on the Internet was available for all to see.

Emerging from the discussions it could be seen that young people took care to evaluate websites asking for personal information to determine whether that information should be divulged.

> *"it concerns me how much some websites ask for when I can't see why they would need the information or if a website asks for an email address for what would appear to be to gain nothing particularly. I don't give my information to them."*

Other respondents gave descriptions of how they falsified data, if they perceived that mandatory fields within a web form requested too much personal data. One respondent described their approach to circumvent the requirement for American zip codes.

> *"I've made up an address just to go with it."*

Young people made extensive use of the Internet to keep in touch with their friends, however there were situations where they had bad experiences of being contacted by

strangers. In these situations, they resorted to making use of the software ability to distance themselves, the example was in Microsoft Instant Messenger, blocking the unwanted contact. Whilst many of the young people involved in the discussions had not had any bad experiences whilst using the Internet, there were notable exceptions. Two respondents discussed innocently accessing pornography. One described looking for information about a basketball team, clicking on a link and being confronted with pornography. Another described pornographic material being sent to a hotmail account, which consequently had to be shut down. Three respondents mentioned financial losses, one had an e-bay purchase incident, another discussed how their brother had been the victim of fraudulent credit card transactions through e-bay, the final respondent discussed a prize draw fraud.

> *"It said we'd won something, then we clicked on it and then it says you ring up. So we rang up and then it said, give the bank details. We'd done it before and it's just then she got scammed over a thousand pounds and lost pounds from her bank account. But then the bank could do nothing about it."*

Contact by strangers through instant messaging was mentioned in five different groups. Girls in one group had been recipients of suggestive remarks made by men claiming to have found their email addresses on a website. One respondent described a friend publishing their contact details on a website, with an immediate increase in spam emails being traced to that specific incident. Another respondent described talking through instant messenger with somebody they had understood to be a friend. However, when the friend started swearing, an unlikely occurrence, they felt that the account was being used by somebody else. One female respondent discussed her suspicions when conversing

with somebody she felt was her own age.

> *"This guy, like * he added me and I just accepted him, thinking oh, I don't know who it is. He said he lived far away. He said where do you live and I goes Torquay and he said where's that, and he didn't know. So I thought, everyone knows where Torquay is and he said I don't. Then I said how old are you and he said he was 13. Then he like showed a picture and he looked loads older, and then started saying like loads of weird things to me, so I thought, then I showed my mum and she said there's no way he's like 13...".*

(* marks where names have been removed to maintain confidentiality)

Strangers making contact however was not the only issue raised during the discussions. One respondent described taking part in an online game involving multi-national players, in this situation the predominant language appeared to be French. The respondent did not speak French and therefore could not understand what the players were saying, however they noticed that their name appeared many times, which made them feel somewhat vulnerable.

Following the findings from the focus groups, an investigation was carried out into how many pupils from each of the three schools were to be found on the top three networks. Another objective was to discover how easy it would be to search for individuals for specific schools. Table 5 below gives the percentage of pupils to be found on the social networking websites. The three schools represented in the research were examined and the overall totals enrolled at the school were obtained from each school Ofsted report for this year. MSN Spaces are not included in this table because they do not allow a facility to search for individuals under a school category.

	School 1	*School 2*	*School 3*
My Space	25%	33%	31%
Bebo	72%	37%	36%

Table 5: Students on websites

The search facilities for all three websites have changed since 2006 when this research was originally carried out and the observations made below illustrate how dynamic this field is. For My Space, in 2006 it was easy to search for people by school, allowing a search for young people between the ages of sixteen and eighteen. On revisiting the site in 2007, the search facility on My Space alters according to the age of the individual logged in. Those under 18 can search for individuals aged sixteen and above, those over eighteen can only search for individuals over eighteen. In 2006, Bebo did not allow searching for young people at a specific school, unless you were invited by somebody already a member of that school group. In 2007 this was found to be different in that the researcher could join any of the school groups without an invitation. MSN Spaces was under development and launched in 2006. In 2007, there was no facility to search according to school. As illustrated in section 2.6.1 , Facebook has increased in popularity and as such deserved examination for its' approach to access to school networks. Facebook allows access to school networks for two weeks before removing the user from the group if they have not been accepted by another member of that group. The changes that the major social networks have made to their privacy approaches illustrate the rapid changing nature of the field, Facebook's response to the privacy concerns to their Beacon application is another such example [Beaumont, 2007].

5.3 Discussion

Use of the internet is a rapidly changing field and the statistics given above represent a moment in time, mid 2006. These values and categories of usage will change over time, and has already been seen with reports of emails and blogs decreasing in popularity towards the end of 2006 [Lev-Ram, 2006; Noguchi, 2006], and with social networks and the use of virtual worlds increasing in 2007 [Kiss, 2007; Metrics, 2007].

As discussed by Bryman [2004] ensuring that qualitative research is both reliable and valid requires ensuring that it is both trustworthy and authentic. To demonstrate these two elements required ensuring that important elements of trustworthiness, credibility and transferability, were present. This was demonstrated by engaging with three different populations in order to gain multiple accounts of their social reality in terms of privacy risks. In addition, two validation exercises were carried out, thus exploring the integrity of the research performed. The first of the two validation exercises was a small messenger survey conducted to ascertain if similar findings emerged from a different population and source of data. The second exercise was to verify the accounts given within the focus groups by searching the social networks utilised by the young people.

5.3.1 Messenger Survey

The survey was conducted amongst users of Microsoft Messenger and utilised snowball sampling. The purpose of the survey was:

- to determine what personal information young people were happy to divulge through the profile facility of Microsoft Messenger;
- to discover if anybody had any reason to regret giving out personal information.

The questions asked about the information that individuals divulged through the public profile directory set up as part of using Microsoft Messenger. Individuals were also questioned about how safe they felt the information was.

There were thirty-two responses, with an average age of seventeen years, an age range between fifteen and twenty-five years old, with 44% being female. The important elements of the responses are summarised below in Table 6.

Question	***Percentage***
Happy to divulge gender	94%
Happy to divulge name	78%
Happy to divulge age	78%
Happy to divulge email address	66%
Not regretted posting personal information on web	59%
Not happy to divulge phone number	59%
Not happy to divulge address	53%
Posted photographs	53%

Table 6: Responses to messenger survey in percentage terms

Whilst the majority of the respondents were happy to divulge their gender, it was interesting to note that all the male respondents were happy but two of the female respondents stated that divulging that information would depend on the context. It was also notable that two male respondents regretted posting personal information on the Internet, no female respondents regretted it with four stating it was not relevant. Posting photographs on the web illustrated an even gender split with half of the female respondents having posted photographs of themselves online, and just over half of the male respondents doing so too. Context was important, with both genders considering

that divulging of phone numbers and addresses was dependent on context.

5.3.2 Web validation

One potential disadvantage of the focus group approach to gathering information, was when considering the interaction between the focus group participants and the researcher. The researcher was entering schools or youth groups as an adult, and as such there were certain social norms that would bear upon the discussions. It was entirely possible that the young people would provide information that they felt was expected of them by an adult, rather than as a true reflection of their social reality. With three of the focus groups, the researcher was known as a youth leader to the participants. The culture of this particular youth organisation bears some relevance, in that young people and the leaders strive for a culture of equality, and acceptance. Young people are encouraged not only to question their social world, but are supported and valued in their contributions to discussions and debate. This means that the interaction between the young people and the adults within their group is very different to that of a group within a more formal environment where adults demonstrate and exert their position of power over the young people. The other focus groups, where the researcher was not known to the participants, also included a youth group with a more formal structure and schools. Here, the researcher was treated as somebody with the authority expected of an adult.

To explore the possibility that the discussions with some of the teenagers within the focus groups might bring some anomalies, further details were sought on the social networks and Internet. In one case, the respondents in one discussion group gave descriptions of their interactions with the Internet which did not match the findings on their social

networking profiles. Two girls had chosen to claim they were older than they really were and had posted photographs online, both actions they had denied taking in the discussion.

These findings illustrate quite nicely how with a mixture of web presence analysis, the findings from the qualitative discussions mix together to help inform further theory. The qualitative approaches alone have their failings, but with a combination of validation exercises that embrace the technology, those failings can be addressed.

5.4 Coding

Coding of the data was carried out by systematically analysing in turn each of the interviews, focus group discussions, word-storms and workshop findings. The approach was to examine the different ways in which the individuals and groups had articulated risks, and to extract the elements that appeared to be of potential significance. Open coding was used initially to break down the data into the categories, through the process of examining, comparing and conceptualising the data. Selective coding followed, whereby the core category was refined and systematically related to the other categories, thus refining it further.

The categories identified were terms given to the impact from damage to personal privacy. This highlighted where the threats to giving out personal information lay and where there was potential for unwanted intervention. These categories are illustrated in the Figure 8 below and feed into the creation of the taxonomy of threat. The taxonomy is presented in the next chapter.

Figure 8: Main concepts arising from research

Four main categories emerged from the data, E-Sociability, Data Confidence, Access Control and Technological Impact. These were further subdivided into related categories as people described the risks they perceived in their interactions.

E-sociability centred around how people viewed risks in terms of their interactions with their peers. Within this category consideration was given to the actions taken in trying to identify bona fide senders of electronic communications. One example was valid invitations to join social networks compared to automatic invitations sent out when an individual joined a network. These automatic invitations, along with other emails and communications generally considered to be spam, caused irritation amongst some respondents. Within one group, the respondent denied they had initiated the action. Given that it was not altogether clear that some of the social networks were going to generate invitations from the individual's email account address book, this claim was not entirely without foundation. One example is My Space, which issues an email invitation to join My Space if a person searches by an email address which does not exist already on My Space. This is not made explicit in the search and can easily be overlooked by the individual searching. Emerging from this irritation factor, was the method of control that individuals took to deal with the situation, primarily that of deleting and ignoring the emails. Further within this e-sociability category, were elements of trust. Trust formed an important role when joining social networks, respondents stated that they would trust their friends and accept the invitations to join the networks due to that trust.

The data confidence category illustrated how respondents put boundaries around the

information they found or gave out. The way that false information was utilised was expressed by some respondents along with the elements of information that were felt to be important and needed protecting in some way. The important pieces of personal information to emerge were name, postcode and nicknames, and photographs. Questions were raised about the way that information was gathered and the design of collection mechanisms. Excessive information was questioned and circumventions applied. Circumvention methods described were using multiple email addresses, withholding information and ensuring that information was given out to established sites rather than new websites. The potential for harm was acknowledged along with the usefulness of the privacy enhancing technologies in protecting personal information.

Access control considered in more detail who or what was allowed to cross the boundaries to personal data already expressed in the earlier category. The decisions made to allow or deny access were also addressed in this category. Blocking and the use of profiles were utilised. Profiles provided measures for security, allowing certain elements of information to be locked out of certain profiles, they also allowed monitoring of who was viewing that information. Ceasing to use a website and forgetting about it was highlighted, whereby individuals had given out personal information, signed up to the website and because they did not use them on a regular basis they had forgotten what they had divulged and why they had signed up to them.

Technological impact considered how the technology altered the individuals' behaviour in relation to privacy. Much of the technology was considered to be very useful to keep in touch with peers, My Space for example was considered as a very useful tool to allow

others to know what the individual was like, and to allow free expression of the individual. Surveillance from technologies emerged as a category of concern, especially from mobile phones in terms of tracking. Bluetooth was mentioned as an issue both for transmitting pictures between peers and as a tool for broadcasting information, for example putting personal name in the device name and making it discoverable. Contact from strangers was highlighted especially in relation to some respondents having their email addresses advertised. Mention was given to government campaigns and the effects they had on the individuals' behaviour. Powerlessness was another issue raised, whereby the respondents did not entirely understand the technology they were utilising and the risks that could emerge from that use.

These categories formed the basis for the taxonomy of threat introduced in the next chapter. They allow for a framework to be utilised for other individuals to consider how the technology they are utilising may bring about a risk to their privacy.

5.5 Conclusion

Gathering information about the risks faced by the three separate populations required adapting the research methods to gain the best fit. This combination of qualitative and analysis of web presence proved a useful approach to include both social and technical factors to explore and provide validation for the findings.

Of the findings, individuals were the most ambivalent of the respondent populations. Whilst some were unsure of exactly what information could be gleaned about them, the majority showed little concern about the findings. The interactions with the service

providers for the Survivors however, showed much more concern and anxiety on behalf of the Survivors. The overall consensus was that whilst the privacy risks uncovered were not completely new, the ability to control the risks had either been removed or changed. Teenagers gave the impression of being aware of what the potential dangers were, and felt that the messages from the education campaigns for keeping personal information to themselves were not entirely relevant because of the trust they held in their friends. In some cases, however, their actions did not match their discussions.

The categories of risk areas that emerged from gathering together all the responses from the three populations, provided a useful framework within which to examine other situations for potential risks. This framework forms the basis of the taxonomy of threat that is introduced in the following chapter, along with a discussion as to how technology may be designed to demonstrate how the risks to individuals might be mitigated whilst providing them with the ability to engage with the technology.

6 Mitigation of risk

This chapter evaluates existing taxonomies for use in risk assessment prior to introducing the second objective of this research, a novel taxonomy of threat created from the concepts emerging in section 5.4 . The chapter concludes with the taxonomy tested by applying to two separate areas of social networking applications and mobile phone usage in schools.

6.1 Introduction

Previous chapters in this thesis have outlined how risks arise (chapters 2 and 3) and how understanding risk should be key element within privacy protection to address social inequalities ([Raab, 2003] in sections 3.3 and 3.5). Lachoee et al [2006] echo this requirement by suggesting that more focus should be on quantifying and addressing risk within the social context, allowing for:

> "education and assurance [to] underpin confident use and informed decision making in ICT use" [Lacohee et al, 2006].

However, risk assessment is not a straight-forward activity. The difficulties for risk assessment arise through the subjective approach of the individual, after all it is a human being carrying out the risk assessment. Mention has already been given to the concern of Furedi [2002], that fear of affecting the future means that risks have no boundaries. Combine this with the unknown nature and potential unknown uses that Internet technologies bring, and there is a high potential for disagreement between risk assessors in addition to difficulties in forecasting the risks. This complex area of risk assessment was discussed earlier in section 4.5, outlining how one risk assessor may view the type of

risk differently from another prior to formulating a plan to remove or minimise the risk.

Mitigating risks, therefore, would benefit from the use of a framework to assist the assessors, to ensure that the relevant areas were considered and to support the decisions made. A taxonomy provides a useful framework when carrying out this type of assessment. The organised structure serves as a lens through which to classify and understand a body of knowledge [Carr, 1993]. Risk concepts can be logically ordered into groups and categories allowing the preventative measures to be applied.

6.2 Existing taxonomies

Existing approaches to categorising privacy threats were not designed to specifically address risks for vulnerable individuals. Therefore, they have their limitations in the context of this research. These taxonomies either focus upon the areas of design, behaviour or legal redress. There are four relevant taxonomies, at the time of writing, and these are described in turn below.

The first taxonomy presented here has been introduced by Solove [2006] who has a focus from the US legal perspective. Solove's taxonomy was designed as a framework to guide legal decisions about privacy law, by providing an understanding of the harmful and problematic activities that are socially recognised. There are four categories to this framework, all based around the data subject, an individual whose life is directly affected by the activities encompassed within the four categories. These four categories are as follows:

- Information Collection: This encompasses all activities surrounding surveillance, the watching, listening, recording, questioning and probing of an individual for information;
- Information Processing: This considers the storage, combining or aggregation of any data linking to the individual. It also covers the protection of the data, secondary use without consent and exclusion whereby the data subject is not allowed to know or have access to information being utilised about them.
- Information Dissemination: covers breaches in confidentiality, the breaking of promises not to disclose information to others, disclosing or revealing information that impacts the way that others may judge an individual. It also covers exposing information about grief, nudity or bodily functions. Amplifying the accessibility to information, using the information for blackmail, mis-appropriating personal data to carry out Identity Fraud or distorting the information so as to mislead people are all included in this category; and
- Intrusion: considers the area of intruding into an individual's private affairs so as to disturb their solitude or tranquillity. Decisional interference is also included whereby others affect the decisions that an individual makes about their own private affairs.

Solove's taxonomy contains wide categories and whilst it may serve some useful purpose to identify in very broad terms where dangers might lie, it is not fine grained enough to transfer to software design in the context of this research. The "Privacy Goals Taxonomy" from Anton and Earp [2002] however, is aimed at website designers, encouraging them to ensure their requirements design protects consumer privacy. The primary focus is on business data and categorises existing threats to consumer privacy into seven categories:

- Monitoring;
- Aggregation;
- Storage;
- Transfer;
- Collection;
- Personalisation; and
- Contact.

The purpose of the taxonomy here is to ensure that the website design acknowledges the dangers in these different areas and seeks to minimise the problems that consumers will face. In comparison to the taxonomy by Solove introduced above, the approach is a little more fine-grained and therefore more suitable for design, but still does not entirely suit the context of this research because of the business focus.

The third relevant privacy taxonomy is the "Privacy Taxonomy" created by the Government of Alberta [2003] to ascertain how privacy enhancing technologies within the organisation manipulate and interact with personal data. This taxonomy has been designed to extend the current P3P initiative by the W3C [2006], to be more relevant to a Government department for use in new applications or database structures. The P3P approach had been identified as not robust enough to assist with the development and expression of privacy policies within government organisations, and so the taxonomy was created. The taxonomy considers:

- the source of the data, whether or not it arises from the individual or a third party;
- the intent of collecting the information, how long it is likely to be kept for, how easy it is to identify the individual;
- the conditions it has been collected under; and
- the consequences of that collection.

Moving away from policy making and design issues, the Cyberspace Research Unit has designed a taxonomy of threat focusing upon the problems faced by children and young people [O'Connell and Bryce, 2006]. The focus here is on understanding the influences in terms of physical, psychological and social well being. There are five areas identified as posing a risk of harm to children and young people. Within each of the five areas, harmful and illegal behaviours are identified, as aids to understanding the degrees of harm that might occur. The categories are illustrated in Table 7 below.

	Commerce and Information	***Social Network***	***Sexual Health***	***Sharing Perspectives***	***Mind, Body and Spirit***
Risks	Misuse of personal information	Offence	Pornography	Aggression	Pro Ana
	Misinformation	Hate Cults	Non-Consensual	Addiction	Pro Mia
	Spam	Racism	Violent	Cyberbullying	Pro Self Injury
	Violations of rights to privacy	Xenophobia	Racist	Happy-Slapping	Pro Suicide / Assisted
		Violence	Fetishistic		
Proscribed	Violations of human rights	Low and high level crime	Low and high level sexual crime	Injury	Incitement to commit suicide
	Advertising Standards	Racially motivated crime		Abuse	Murder and attempted murder

Table 7: Cyberspace Research Unit - Taxonomy of Risk

Each of the taxonomies introduced above, whilst having some bearing on relevance on the research space, have not been designed to address the specific issue of risk assessment from the dissemination of personal information and appear to contain very wide ranging categories. Therefore, although elements can be useful and lessons learnt from them, a taxonomy devised with a focus on the research space presented in this thesis will have more relevance and be more suitable.

6.3 Taxonomy of threat

The taxonomy is created from an understanding of the categories that emerged from the coding exercise described in section 5.4 , where respondents' views about where threats

arose were considered. These acted as useful frames within which to ascertain how devices and situations manifested threats to individuals. Cross referenced with these categories were risk categories identified in terms of the potential impact where damage to personal privacy could take place; where risks to giving out personal information might lie; and where there was a potential for unwanted intervention. These three areas are extracted from an understanding that privacy is:

- protection from harm,
- control over personal information and
- freedom from unauthorised intrusion.

Within these three areas, the manner in which the risks to individuals manifested themselves are considered within the four different categories, which are repeated here:

- e-Sociability: This focused on the act of being sociable within the electronically connected context and examined the methods employed for keeping in touch with peers.
- Data boundaries: How individuals determined which elements of personal data required protection and how boundaries were created around personal data.
- Access control: Consideration given here to how boundaries around personal data were enforced, along with levels of empowerment and tools to enforce the boundaries.
- Technological Impact: The effects of technology upon the individuals' behaviour.

This taxonomy is illustrated in Table 8 below and examples of its application are illustrated in section 6.4 - Evaluation .

	a) Propensity for Harm	***b) Divulging Personal Information***	***c) Unauthorised Intrusion***
e-Sociability			
Data Boundaries		Device functionality	
Access Control			
Technological Impact		Manifestation of risk	

Table 8: Taxonomy of Threat

6.4 Evaluation

This taxonomy has been validated by testing out how it can apply to two separate situations. In both situations the investigation considered media reports, literature and direct evaluation to understand how the taxonomy could highlight potential risks. Both situations have been published at peer-reviewed conferences. The first area considered social networks [Atkinson et al, 2007] and the second considered mobile phones within the education environment [Wood et al, 2007]. These situations are individually discussed below and cover some of the literature already discussed in chapters 2 and 3 .

6.4.1 Evaluating threats from social networks

Social networking web applications allow individuals to link to each other and give a good example of uncontrolled data exchange. Something divulged to one friend with a direct link to the individual could be observed by somebody else who does not have a direct link. Social networking applications were considered a suitable area for examination due to the concern raised in Wired News [2006] where posting information on such a website had been linked to murder.

Five social networking applications were considered for this investigation and will be referred to as a collective of "social networks":

- www.myspace.com;
- www.bebo.com;
- www.spaceslive.com (Windows Live Space);
- www.facebook.com; and
- www.zorpia.com.

These applications were sampled from those listed by teenagers in the questionnaires described in section 5.2.3.1 5.2.3 . A summary of functionality and associated threats is displayed below in Table 9.

	Propensity for harm	*Divulging personal information*	*Unauthorised intrusion*
e-sociability	Personal data gleaned for use in situations of bullying, stalking and harassment.	Photographs, blogs, journals, discussions linked to personal profiles. Name and address used in search and display terms.	Photographs and video's uploaded by third parties. Access to profiles through friends rather than directly
Data boundaries	Linking postcode to mapping applications. Linking date of birth to GRO indexes to obtain mothers maiden name.	Profile made public. Third parties divulging information.	Third parties posting photographs, names, addresses and other personal details.
Access control	Search on location, gender, age.	Control of profile vs finer grained control of individual data elements. First name and photograph returned in search.	Tagging and linking of photographs. Searching
Technological impact	Lack of safety warnings on some sites	Important personal information mandatory for registration	Data control rules applied from different country.

Table 9: Summary of functionality and associated threats from Social Networks

6.4.1.1 E-Sociability

Social networks are one of wide variety of Internet-mediated communication methods. "Blogging", creating on-line diaries, is considered by the BBC [2006c] as a growing phenomenon, however it remains to be seen if that is the case. However, CEOP has raised this phenomenon as an area of concern whilst McMillan and Morrison [2006] observe how young people build their community around these interactive technologies. Gross et al [2005] suggest that the interface of social networks combined with peer pressure, herding behaviour, and short-sighted privacy attitudes contribute to the situation where young people reveal quantities of personal information. The convergence of technologies also encourages the sharing of information, as discussed in chapter 2. Nokia

phones with the LifeBlog software; O2 encouraging people to upload content in return for payment [O2, 2006] and YouTube's facility to view their site from mobiles [BBC, 2006b].

Each of the applications considered allowed people to link and connect with each other. Common features included photographs and some form of comment whether in the form of blogs, journals or discussion boards. MySpace, Bebo and Facebook all link people together in groups; these can be based on school, university or the workplace. Bebo and Facebook provide differing levels of control over who joins the different groups. In the case of Bebo you cannot join a group uninvited, another member must enrol you. Facebook allows you access to school networks for two weeks before removing you from the group if you have not been accepted by another member of the group. Bebo, Facebook and MySpace offer a multimedia rich environment allowing music and videos to be shared and played. Zorpia is aiming at the over 16 year old market and does not therefore group people by school or organisation, just by location. Facebook provides the facility to upload photographs and place description tags of individuals within the photographs that link to the personal profiles of those people.

6.4.1.2 Data boundaries

Each of the five websites collect and display a wide variety of personal information, with each providing the facility to post photographs. As a minimum MySpace collects first name, last name, postcode, country and email address. Facebook and Zorpia do not make as much information mandatory.

6.4.1.3 Access control

The approaches and tools for profile protection differ between the five websites. Facebook

is the only website to offer a fine-grained approach to controlling what is made publicly available. Many of the personal data elements can be toggled between "public" or "friends only" viewing. Photographs that are tagged with an individuals' name are notified to that individual, thus allowing them the opportunity to request their removal if required. Profiles and photographs of individuals can only be seen once a link has been made and approved by the other party.

Bebo had a more coarse grain approach to privacy by providing the facility to make the whole profile private only. Each of the websites assessed allow the individual to hide their date of birth, and each allowed the facility to view the friends of connected friends. However Facebook gave only the briefest public profile of those friends whereas My Space and Bebo allowed more detail of the profile to be viewed by third parties.

Searching for individuals differed amongst the websites, some allowed searching for individuals by location, age and gender, others were more restrictive only allowing searching to be carried out on networks that the searcher has been invited into. Zorpia allows searching to be carried out by gender, age and location. MySpace uses first name, last name and location for the searching and state in their privacy policy that pictures and first names will be displayed to users who search for you. Windows Live Space and Bebo provide a free text search box and do not have a facility to refine the search any further.

6.4.1.4 Technological impact

Each of the websites allows and encourages personal information to be shared, however each has a different approach to protecting the users' privacy. MySpace is the only one

to make the majority of important personal information mandatory to join the site. First name, last name, email address, postcode, country and gender are all essential for registration, date of birth however can be omitted. It does provide safety tips and the privacy policy from links at the bottom of the page and the registration page reminds potential users that their data will be stored and bound by US data rules.

Bebo and Windows Live Space make more of the interaction with CEOP and blog safety campaigns by placing the links to report abuse and safety guidelines in prominent positions. Bebo places reminders for those under twenty-one next to the text boxes so that the safety tips are more prominent. Zorpia, being aimed at those over sixteen, carries no such warnings.

6.4.2 Evaluating threats from mobile phones

The next investigation observed the education environment. As outlined in section 2.6.2 , the majority of young people now carry a mobile phone. Mobiles within the education environment pose a number of challenges, not least surrounding the plethora of functions now encased within those mobiles. One challenge for the individuals in positions of responsibility within the education environment is that they need to be aware of the threats posed to young people from the use of mobiles and from there to take appropriate action. A summary of the potential threats is given in Table 10 below.

	Propensity for Harm	***Divulging Personal Information***	***Unauthorised Intrusion***
e-Sociability	Device functions: Text, Camera, Phone calls, Email, Blogging, Bluetooth. Manifestations: Bullying, abuse		
Data Boundaries	Device Functions: User-controlled: Text, Camera, Phone calls, email, blogging, Bluetooth. Manifestations: Third-Party: Location based services, surveillance		
Access Control	Change SIM card Contact Service provider Location based tracking services Unfair charging strategies		
Technological Impact	School policies on mobile phones Examination procedures 'cheating'		

Table 10: Summary of risks posed from mobile phones

6.4.2.1 E-Sociability

Each of the six methods identified above for e-sociability, namely: text; phone calls; camera; bluetooth; email; and blogging have the ability to be abused by individuals to bring about harm to another individual. They also blur the boundaries between the other two elements in the taxonomy, divulging personal information and unauthorised intrusion. Primarily the threats manifest themselves in terms of mugging; bullying; and predatory behaviour.

As discussed in section 2.6.2 , mobile phones offer a wide variety of different methods for interaction: text messaging; image messaging; phone calls and email. Text messaging has been identified by Devitt and Roker [2006] as the preferred medium for communication. Bullying and video clips of violence, sometimes termed "happy-slapping" are not the only concerns. A substantial number of young people had experienced

unpleasant incidents with mobile phones which included theft and mugging along with bullying and "happy-slapping" [Devitt and Roker, 2006]. Bullying of both pupils and teachers has been raised as a problem. In 2005 Goodchild and Heathcote [2005] reported text stalking cases to have reached one million per year with 5,640 prosecutions under UK harassment legislation introduced in 1997. NCH quoted figures of 14% of young people being affected [Catan, 2006]. Field [2006] describes text bullying as being the result of a combination of factors to provide anonymity to the bullies; an increase in the number of young people owning a mobile phone; telecommunications service providers being slow to react; and weak laws.

Cameras embedded within the devices provide high resolution to take clear digital photographs and there is the ability to record short video clips. Pictures are easily transmitted because the cameras are embedded within the mobile phones, the mobiles are small and quite discreet and providing the sound is turned off nobody knows the picture has been taken. Those pictures can be easily transmitted to others or uploaded to the web.

Bluetooth along with Wireless (Wi-Fi) connectivity provide different methods of transfer of images at little or no cost to the owner of phone, making them an attractive choice for sharing pictures with friends. To use Bluetooth, two devices must be paired together. However, once two phones are paired, the receiver has no control over the images or files that they receive. Another issue surrounds the potential for security vulnerabilities which could allow malicious code to be run on the mobile phone [Zetter, 2004].

New phones provide the ability to watch videos and some like the Nokia N73 allow videos to be downloaded. As mentioned in chapter 2 , mobile phones allow interaction with social networking websites and therefore bring with them the risks posed by those environments, as discussed in the section 6.4.1 .

Web access is made easier from the mobile phone with the use of General Packet Radio Service (GPRS). This allows charging by amount of data consumed rather than per connection, thus making Internet connectivity cheaper. Email can be collected whilst mobile using this type of connection or the bluetooth or Wi-Fi mentioned earlier. The cost of sending information to social networking websites is reduced by connecting the phone to a computer.

6.4.2.2 Data boundaries

Controlling where personal information is divulged becomes more complex with the influence of mobile communications. There are two main influences, user-controlled sharing of information and third party. As mentioned in the earlier section on e-sociability, sharing of personal information can be facilitated easily but it can also be controlled with the functions on the mobile phone. However, it is the third party actions, intruding upon the data boundaries of other people that are the primary concerns.

Transforming the mobile phone into a surveillance tool has become easier. Software can be downloaded to transform a mobile phone into a surveillance camera [Smart Card Group, 2006] and voice analysis software can be used to monitor phone calls and advise on predominant emotions [Power, 2006].

6.4.2.3 Access control

Controlling who has access to an individual through mobile communication relies upon the techniques designed into the device and the policies adopted by the telecommunications providers. Should an individual be experiencing problems and wish to change their mobile phone number, they have two options, one is to change the SIM card within the device for a relatively small sum of money; the other option is to approach the service provider and ask for a number change. Currently there is no facility on the device to block specific individuals from contacting the user.

With location tracking services, the user of the mobile phone is expected to have agreed to accept location tracking on their mobile. This comes in the format of a reply to an initial text message, which is easily deleted from the phone's memory. Reminder text messages are sent during time periods that vary between 14 to 31 days. However, Rootsecure [2006] describe how to overcome these protection methods.

6.4.2.4 Technological impact

The impact of mobile phones on the school environment has already set in motion events to put policies of use into place with some schools developing policies to set out their expectations with regard to mobile phone use. In general, such policies identify theft, bullying, unauthorised use of image capture and potential disruption to discipline as the areas for concern. Whilst it is recognised that these issues constitute clear threats to the safety and security of individuals within the school, it is equally clear that the less obvious threats associated with access, tracking and where data boundaries lay are not included.

In data collected by Wood et al [2007] some instances were found where teachers

reported incidents arising from inappropriate use of the camera facility on a mobile phone which prompted the school to collect all mobile phones from children as they entered the school and return them at the end of each day. Such actions create management and organisational challenges for small schools and would be prohibitive in large schools.

For the majority of schools, the development of a policy which states that mobile phones are not to be used during the school day provides the only means of protection from the potential of inappropriate use. Teachers report that this has not prevented incidents where mobile phones have been used to facilitate bullying with unsolicited images being captured and distributed.

As pointed out by the British Educational Communications and Technology Agency [BECTA] 'The dangers associated with a standard PC regarding unsuitable material apply to mobile phones and other devices too, yet because mobile phones are personal and private devices, it is not always possible for parents or schools to monitor their use.' [Becta, 2004].

6.5 Conclusion

This chapter has explored how the concepts arising from the data collected from the participants can be incorporated and understood for use in a framework for further understanding. By turning the underlying concepts into areas illustrating useage, a taxonomy has been created. For example, the link between how young people used blocking to control who they interact with, led us to explore how access control was delivered in the technologies in use. This in turn allows for a risk assessment to consider

what is provided in this area.

Within this chapter, the utility of taxonomies for use in risk assessment was established, in addition to addressing some of the problems encountered in the risk assessment process. An examination of existing taxonomies discovered a focus on either the business or legal domains which were not entirely suited for the respondent groups selected. A taxonomy matrix was created whereby evaluating the intersections between the categories led to uncovering potential threats. Validation of the taxonomy involved investigating the two specific areas of social networking applications and mobile phones in the education setting. The investigations allowed for the taxonomy concepts to be explored in more depth and allowed a brief summary of threats to be illustrated for the two areas. The next step is to integrate the findings highlighted for the taxonomy into a design for software, so that technology can serve the individual in minimising risk.

7 Software Design

This chapter introduces the third objective of this research by outlining the requirements for the prototype software and a design specification created. Three achievable pieces of functionality are selected to explore in more depth. This chapter details how the Vulnerability Assessment Framework is created along with a discussion on the pertinent elements of the Semantic Web. This chapter concludes by introducing the conceptual architecture for the software prototype.

7.1 Introduction

The next stage of this research was to take the understanding of risks along with the resulting taxonomy of threat and move towards creating a privacy-supportive environment. Careful consideration was given to how this might occur given the complexity of the privacy context, the levels of empowerment for the participants and current technological limitations. The choice was narrowed down quite specifically to creating a browser plug in, a piece of software embedded into a browser.

The browser was chosen as it provided the primary outlet for personal information. This was certainly seen with the teenagers in the focus groups, introduced in section 5.2.3.1 . Young people gave out personal information when signing up to websites and when communicating with friends. Within the refuge situation, as reported in section 5.2.2.1 concern was raised about how the Survivors were giving out not just their own personal information, but that of other Survivors within the refuge.

7.2 Design Objectives

The objective was to design a browser plug in to allow the individual to control their personal information and that could be tailored to the context of the individual. A set of objectives for the prototype were devised from the discussions held with respondents in combination with the literature introduced in chapters 2 and 3 . These objectives were:

- to provide an environment which would facilitate individuals linking their actions to the consequences of their actions;
- to encourage the individual to be proactive in controlling the flow of their personal information by providing an environment where they could monitor where their personal information was being given out;
- provide a simple and easy to understand interface;
- to not require explicit choice of protection.

The first of these objectives, addresses one of the criticisms levelled at the use of PETs. By allowing the individual to review their actions, explicit links would be made by the individual to the consequences. For example, by reviewing the amount of personal information divulged, the individual would be able to see just how much information was being made available by their own actions.

The second objective, to encourage the individual to be proactive in controlling the flow of their personal information, addresses some of the issues encountered by other approaches to risk reduction. For example, Livingstone and Bober [2005] highlighted the issue whereby rules and monitoring were unpopular. The focus groups' discussions with

young people echoed this view, voicing frustration at the blocking software utilised within the school environment. The objective aims to increase only very slightly the cognitive friction involved for the individual when giving out their personal information. By making it slightly less easy, by increasing the relative difficulty of the task and the mental capacity required to complete it, the individual will be more aware when giving out their personal information. Suchman [1991] discussed the concept of situated action, where the actions that users take are based upon their understanding of their environment, and if their understanding is incomplete, there is the tendency to make assumptions to fill in the gaps in their knowledge. Hine [2000] also outlined how an individuals' belief about the Internet influenced the way they interact with it. Creating the facility for the individual to be responsible for giving out their own personal data will also take some steps towards addressing the issues of lack of knowledge or power faced by individuals when attempting to control their information [Stahal, 2004].

For the prototype to be successful in achieving its' objectives, a simple and easy to use interface that reduces the individual's information load is required. However, this is an approach that would appear to go against the second objective, where the cognitive load of the user was increased. The purpose of the prototype is that the information being communicated to the individual should be easy to assimilate and understand, with representations meaningful to the individual being incorporated into the interface.

The final objective addresses the criticism raised about PETs requiring explicit choice by the individual, which may be misguided. Achieving this objective required that the prototype be an integral part of the software tools already in use by the user. Therefore

part of the implementation criteria was that the software be integrated into the browser.

To move from the objectives of the prototype towards a workable design, consideration was given to the requirements of the end-users. This involved consideration of three actors viewpoints:

- the individual: anybody who could make use of the software directly for themselves;
- the support worker: includes individuals who support vulnerable individuals and are seeking to provide protective assistance for individuals who might not be able to access the system for themselves; and
- the organisation: any specific body that has a moral or legal obligation to protect a group of vulnerable individuals. Examples here could be refuges or schools.

Achieving the above objectives formed the element of the research that addressed the action for change, as outlined in section 4.2.1.4 . Participants' views were incorporated into the design of the prototype, and indeed they were to be consulted again once it was implemented which is reported later in chapter 9 . However, this is where the similarity to action research had to end. Because the participants either represented Survivors or were teenagers, levels of empowerment and access restrictions meant they could not play a more active role in the design process. These were not the only restrictions, financial and time restrictions were also in place.

7.3 Functionality

The next phase was to design in more detail how the software would address the

objectives outlined above in section 7.2 , but in a way that would be achievable within the limited timescale in place. Three primary pieces of functionality were identified and decomposed. These were:

- *to manage privacy settings* – The overall objective was to provide the means for the individual to determine how they wanted their information to be protected. A list of questions would be posed to the user to collect details about their protection needs. These answers would gather the information including: gender; name; address; and work location and would utilise the Vulnerability Assessment Framework (VAF), described later in this chapter. A weighting for the elements of personal information would be stored as preferences, upon which further computation would be carried out. A facility to amend questions is also be included.
- *to receive threat notifications* – The software would notify the individual about any potential threats to their privacy. A search facility within the software would notify the individual of websites containing their personal information. New emerging privacy threats would be communicated in a fashion determined by an evaluation algorithm. The evaluation is based upon the Taxonomy of Threat in combination with the VAF, thus tailoring the notification preferences to the individual.
- *to manage personal information divulged to websites* - This would record where personal information is given out, providing for threat notification functionality to demonstrate to the user how much and where their personal information had been divulged. Additional monitoring would include other individuals within the organisation, for example other residents within the refuge.

The features that would best demonstrate the achieving of the objectives were determined to be as follows:

- To provide the ability to monitor where information is given out about the organisation and individuals within that organisation.
- To find where information is held on the Internet and to display the URL where it can be found.
- To provide a traffic-light indicator to display analysis of the personal information threat of a webpage.
- To highlight web fields within a webpage that are collecting personal information.
- To display a summary of where personal information has been given out
- To display the details of the URLs where the personal information has been given out.

Observations about the users opinions of these features were used as the primary questions for the evaluation, described further in chapter 9.

7.3.1 Vulnerability Assessment Framework

The VAF framework comprises three main elements. A set of assessment questions, a rating mechanism, and a minimum set of personal information elements that require protection.

The assessment questions are in two sections, personal information and lifestyle, to incorporate elements of both static and dynamic factors that influence an individual. Static

factors, represented in the personal information section, combine the examination of historical and long term characteristics and represent either past happenings or things that will not change in the near future. Dynamic factors, in the lifestyle section, represent elements that could change and would require constant monitoring. The questions within the framework are also based upon the findings from using the taxonomy of threat as presented in section 6.3 , and as such form the next step in the process of risk assessment. Here dynamic factors are accounted for in the lifestyle questions, the principle being that the taxonomy will give indicators as to the areas that have the most potential for risk. The questions will ascertain if the individual is likely to encounter these potential risks. For example, the questions will ask about:

- the likelihood of engaging with social networks, linking to e-sociability;
- sole use of the computer, linking to data boundaries and access control; and
- own approach to technology, linking to technological impact.

Risk assessment, as discussed in section 4.2.3 , plays a prominent role for reducing the potential for harm and the inspiration for this approach comes from the risk assessment tools utilised by the United Kingdom Probation Service. Their current system for assessing risk is the Offender Assessment System, (OASys) bought into use in 2003. OASys encourages a holistic approach, assessing the situation and behaviour as a predictor of the potential for future risk of harm [OASys, 2002]. However, whilst this tool is primarily aimed at assessing risk from the offender perspective, it is utilised to ascertain the risk of serious harm, risks to the individual and to others. It is this approach to risk assessment that has been examined for potential useful approaches to be incorporated

into this VAF. The OASys manual highlights the limited evidence base for effective prediction of risk of serious harm, pointing out that one of the major contributory factors is that the risk of serious harm is not a unified concept, but one that is a conglomeration of different types of risk to different types of individual.

The rating mechanism provides a measure to reflect the propensity for an individual towards vulnerability. This approach may appear strange given the previous discussions in chapter 4 , those surrounding the selection of qualitative approaches, based on the argument that allocating a numeric value to a concept that does not inherently possess a numeric value was not suitable. However, two things are of note here. The first is that the process of establishing the numbers is an important one. To explore what should be given a rating and what elements of personal information need protecting is a process that should be explored further. This process allows for knowledge and understanding to be gained about the importance of protecting personal information. The second thing to note is that for the concept of vulnerability to be addressed within the software, the measure was considered necessary. As discussed in section 3.3 , vulnerability is considered in terms of the effects of privacy breaches. The purpose of the measure was to assess the propensity of an individual towards vulnerability and as such required an understanding about how risks are assessed and managed.

The assessment questions gather information about the likely severity of the consequences of disclosure, along with the likelihood of the event. This provided the input into the assessment algorithm, the output of which is a numerical result to reflect the assessment rating. This is represented in the assessment matrix below in Table 11

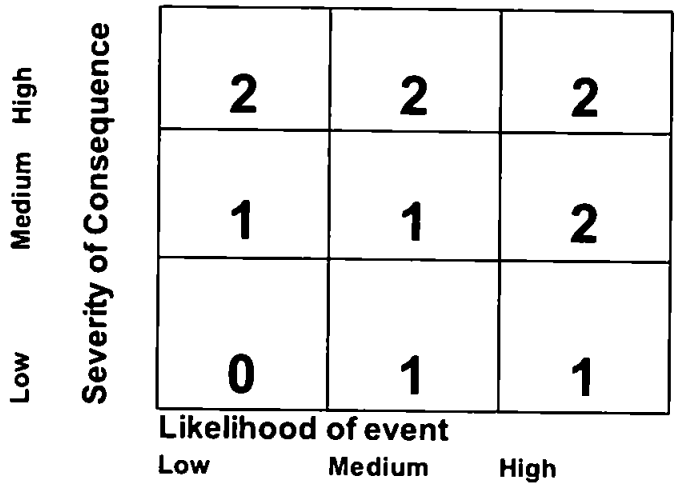


Table 11: VAF Assessment Matrix

The likelihood and severity were considered in terms of Low, Medium and High to select the appropriate rating. A more detailed definition of what constitutes low medium and high is given below in Table 12.

	Severity of Consequence	***Likelihood of Event***
High	Significant physical, mental or emotional injury from which recovery is difficult or impossible.	Event more likely than not to happen. Could happen at any time.
Medium	Significant event from which recovery is quick and/or easy and relatively painless.	Event likely under specified circumstances, which do not exist at the moment.
Low	No significant injury. Serves as an inconvenience only.	Identified as possible in circumstances, but less than likely to come about.

Table 12: Description of severity and liklihood ranks

This simple scoring system echoes the current OASys [2002] approach which found the most effective scoring systems were kept simple. Within the OASys context of the

Probation service, scales beyond 5 points were found to be unworkable and where judgements were required from practitioners, the simple 0,1,2 scale was found to be the most effective [OASys, 2002]. Adopting this simple high, medium and low approach also incorporated well into the choice of a simple traffic-light metaphor for communicating risk to the user of the prototype.

The rating mechanism is applied to a basic set of personal information elements which allows for the potential to be extended. as determined by the needs of the individual. Initially the relevant elements of personal information were determined as:

- Name;
- gender;
- current location; and
- address.

7.4 Architecture

Given the requirements for the prototype, careful consideration followed concerning the techniques and technologies that could be utilised to fulfil those requirements. Creating a browser extension appeared to be the most logical approach to provide seamless integration into tools already used by the individual. Behind the interface, the architecture of the software had to have the ability to combine disparate pieces of information from heterogeneous sources. Therefore the techniques attributed to the Semantic Web were considered to be the most appropriate.

7.4.1 Semantic Web

The Semantic Web offers a new approach to sharing data, although it is not yet mainstream. A Semantic Web application is one that shares, reasons and aggregates structured data allowing simple functions to be automated. Berners-Lee [2000] proposes that the technologies of Extensible Markup Language (XML) , Resource Description Framework (RDF) and Web Ontology Language (OWL) be stacked in such a way that when combined with the approaches of logic, proof and trust, the aim of the Semantic Web can be achieved. The primary goal for the Semantic Web is to streamline the interchange of data [Passin, 2005] allowing for interoperability. As more devices connect through Internet protocols, the automated sharing, aggregation and exchange of data will become more desirable [Davis, 2003]. Individuals will seek to combine the many different ways they already interact with the web, through web pages, newsgroups, and email and will be seeking to use ubiquitous devices and mobile phones [Fensel et al, 2003].

The supporters of the Semantic Web propose that it will solve some of the problems inherent in the current web, problems that include: information overload for the end user; lack of communication between ubiquitous devices [Davis, 2003]; broken links and out of date information [Evans,2001]; and combining legacy systems [Kluth, 2004]. Some authors suggest that the Semantic Web will change the individuals' interaction with the Internet. Cabral et al [2004] envisage knowledge and business service consumption changing. Fensel et al [2003] envisage a wider variety of uses, giving one example of interfaces adapting to end-users communication requirements.

Conceptually the Semantic Web can be viewed from two angles, the creation of content to

be consumed and the act of consuming that content. Authors are required to annotate and describe their data, using clearly defined protocols. Searches utilise these clear descriptions to retrieve the information relevant to their query. XML underpins the standards of Resource Description Framework (RDF) and Web Ontology Language (OWL), all three of which have been issued by the World Wide Web consortium [W3C, 2001; W3C, 2004] as recommendations. Work is still in progress as to how logic, proof and trust are to be implemented.

Figure 9 illustrates how the interactions between the Semantic Web protocols will be achieved. The author creates an RDF document containing triples expressing the relationships of the data held. The triples link to concepts articulated within the OWL ontology document, which is an agreed, predefined set of terms. OWL is a formal language representing the relationships between the terms and relates to a specific domain. These documents are either stored as web pages on a server or could be delivered through a Semantic Web enabled web service. OWL-S is a standard defined to describe web services and combines with the Web Service Description Language (WSDL), giving the web service profile, process model and instructions on how to invoke the service. Consumers access the data either through instructing software agents or by interacting with a web application. Either of these approaches will utilise the commonly agreed ontology to find relevant data accessible through the Internet. The information is gathered from heterogeneous sources and combined presenting information relevant to the context of the end user.

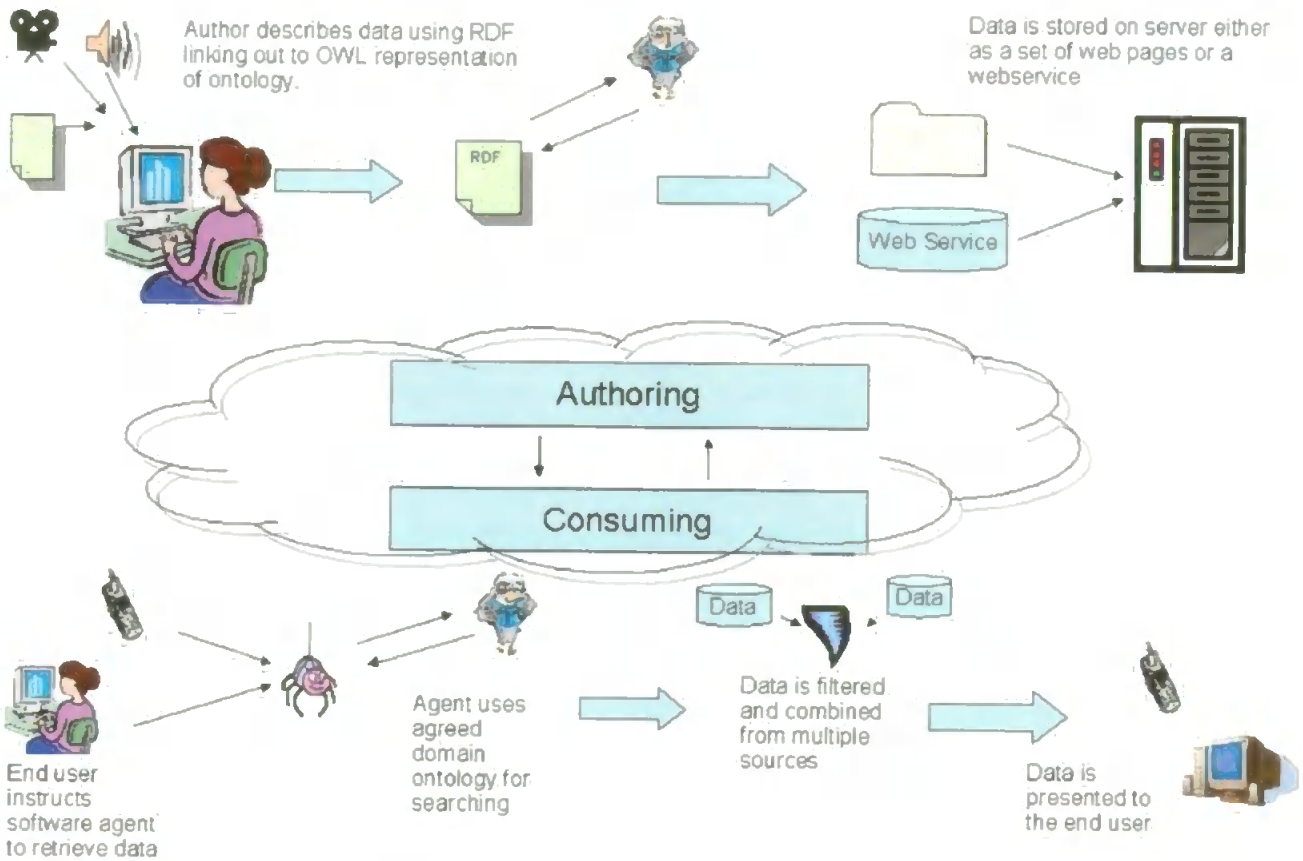


Figure 9: Illustration of Semantic Web Activity

Current Semantic Web applications are aimed at sophisticated expert users manipulating large bodies of knowledge through a personal computer. The Semantic Web approach is very new, and standards that build the architecture as a whole are still under development. The W3C has a working group on a standardised query language for RDF called SPARQL [Miller, 2005]. Other research considers how to design, create and utilise ontologies, creating tools to make this process easier [Harper, 2006; AIFB, 2006; Hudson, 2002; Hewlett Packard, 2006; Altova, 2006]. Working models have been created to demonstrate concepts and include web portals [Wu et al, 2003; Bachlechner, 2006], services and agent based applications [Chen, 2003, 2004].

The Semantic Web proposes to be a way of addressing some of the problems of information overload arising through the Internet. Careful editing and tagging of data will allow manipulation by machines to create context relevant information for the end user. It is this claim that is attractive to this research. The prototype will combine information from diverse sources and present that information to the user in an appropriate and context-dependent fashion. Therefore, the Semantic Web was deemed to be a useful component of the prototype.

Utilising the Semantic Web posed challenges for the development because it is not yet a mainstream or mature approach. Several assumptions were required in order to create a fully working prototype, these assumptions are given below.

- Structured data and relevant linked ontologies would be available.
- Majority of data to be in an accessible format for Semantic Web reasoning.
- Suitable ontologies to be in existence that are easily accessed and utilised.
- Functions from third party Semantic Web applications would be available through Semantic Web services.

7.5 Conceptual Architecture

The following conceptual architecture was considered to provide the most suitable design for the prototype. This incorporated the structured data approach provided by the Semantic Web and the browser interface. The architecture is illustrated in Figure 10

below.

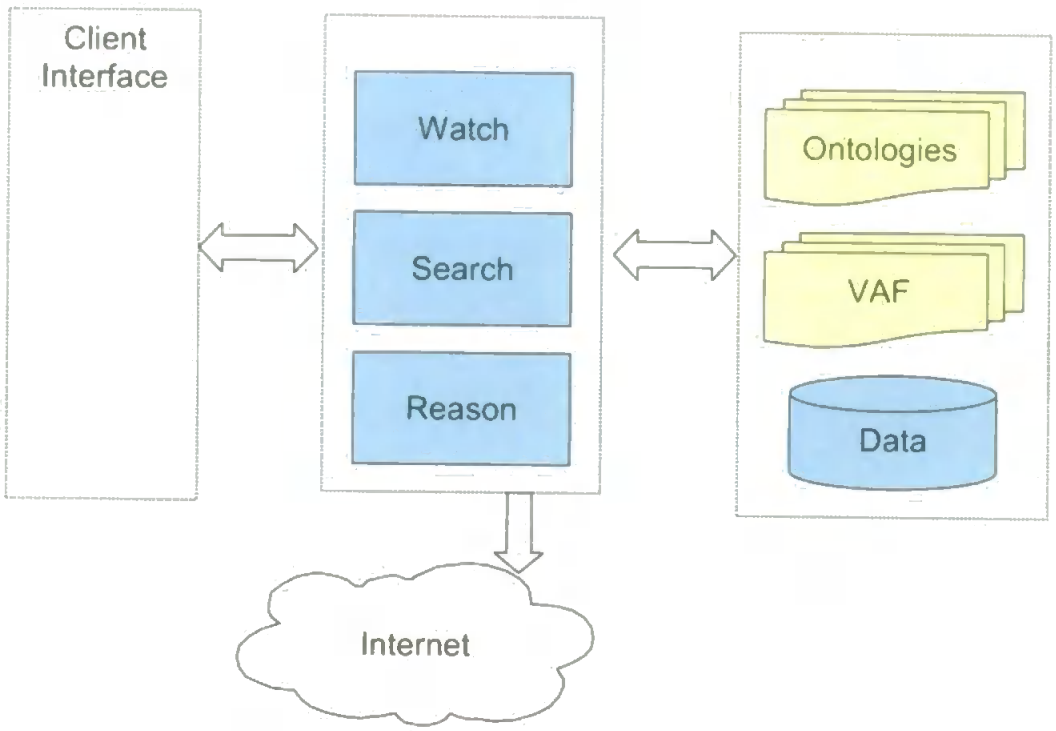


Figure 10: Conceptual Architecture

The architecture provides flexibility to allow the application to be linked to by any client interface. The two browsers, Mozilla Firefox and Internet Explorer, were considered. Both provide facilities to write browser extensions. Mozilla provides flexibility whereby plugins are created using XUL and javascript files and are loaded on started up. Internet Explorer provides libraries where browser helper objects can be incorporated into the main browser.

Linking to the client interface are a set of three components that deliver the core functionality for the application. These are Watch, Search and Reason elements.

The Watch component concentrates on monitoring the interactions with the Internet,

saving details to the data store about where personal information is divulged. To carry this out effectively, it consults stored data held on the same machine. The Watch component interacts with the Reason component to determine the type of alert required to be communicated to the user.

The Search component uses data from the settings to determine what public data is held on the Internet concerning the individual. Details about the findings are written to the data store by this component. Interaction is carried out with the Reason component to provide consequence scenarios by combining the data divulged as stored by the Watch component.

The Reason component forms the central element within the application. Data held in the data store is accessed and used in conjunction with both associated ontologies, and the VAF settings, to reason about data found by the Search component or observed by the Watch component.

The data and the VAF settings are stored in RDF format allowing simple reasoning to take place. Data about the individual is stored on the individuals' machine, but common ontologies used to describe data are referenced externally.

7.6 Conclusion

The third objective of this research required implementing something suitable for mitigating the risks highlighted in the previous chapters, and in such a fashion that supported the

overall epistemological approach highlighted in chapter 4 . Three key pieces of functionality were determined as the most important and the means to achieve these required that a rating mechanism be created. The Vulnerability Assessment Framework was based upon key ideas of risk assessment and provided the mechanism by which ratings could be applied to personal information. The need to combine separate pieces of information was addressed by using key elements from the Semantic Web, an evolving approach that is not yet mainstream. The conceptual architecture was illustrated and described, illustrating how the components of the Semantic Web of RDF and OWL could be used to benefit the individual.

Whilst this conceptual architecture offers a novel demonstration of how risk assessment, situational crime prevention and privacy enhancing techniques can be combined, the next chapter illustrates in more depth exactly how the architecture can be demonstrated and utilised.

8 Prototype Implementation

This chapter describes how the conceptual architecture introduced in section 7.5 was implemented, illustrating in depth how each component was created. The chapter concludes with a demonstration of how the individual can interact with the software.

8.1 Introduction

Microsoft software dominates the home user environment and therefore Internet Explorer was selected as the interface of the prototype. Within Internet Explorer 7, browser helper objects integrate with the browser functionality and allowed for developers to add their software. The prototype was named PSQ and was designed to run on an individuals' machine. The minimum requirements were for a Microsoft Windows XP platform, standard personal computer running Microsoft Windows Internet Explorer 7. All personal data is saved on the individuals' machine. The only time that personal information is utilised externally being as search terms for the search web service. Ontology files, however, are held on a central server, but they do not contain personal information about the user. The programming environment utilised C# along with the .NET platform, with Visual Studio 2005 chosen as the development environment of choice.

The diagram below in Figure 11, illustrates an overview of the code libraries used to implement the conceptual architecture outlined in the section 7.5 . Each of these elements is discussed in turn below.

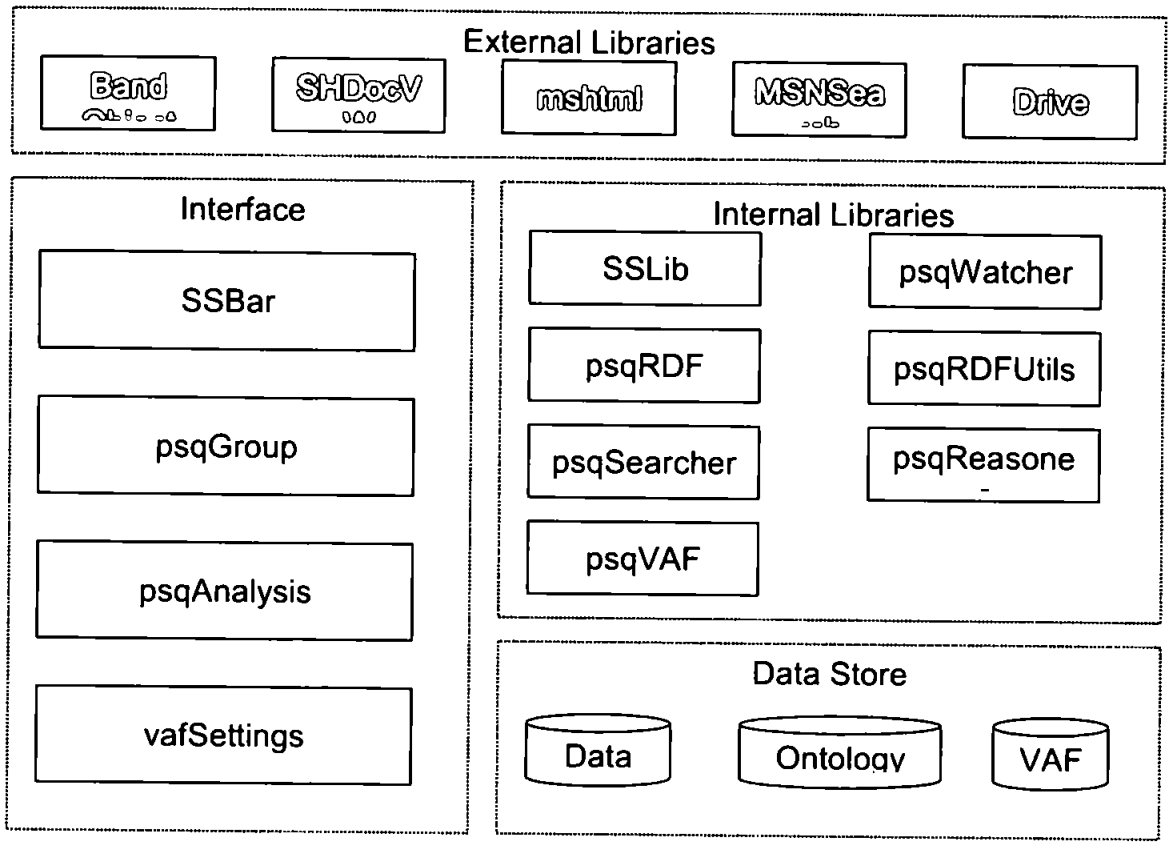


Figure 11: Implementation libraries

8.2 External Libraries

The prototype is based on the Browser Helper Object (BHO) in Internet Explorer (IE) 7 and is created from windows control project, SSLib, that inherits from the external BandObject library, loaded from the Microsoft MSDN website [MSDN, 2007]. The Band Object is a COM component utilised by both Windows Explorer and Internet Explorer. SSLib requires a strong name to be created prior to registering the component using the following post build instructions for the project.

```
cd $(ProjectDir)..\bin\Debug
    gacutil /if SSLib.dll
    regasm SSLib.dll
```

The toolbar interface in Internet Explorer is created by SSBar inheriting from the SSLib library and is described in the next section, 8.3 . The SSBar accesses the external libraries of Interop.SHDocVW and Microsoft.mshtml to process the webpages loaded into the browser.

Two of the internal library components, described in more details in section 8.4, accessed external libraries, psqSearcher utilised the webservice provided by MSN API [MSDN, 2007a], and psqRDF accessed Drive. To make use of the MSN API, registration is required to gain a unique user key. Drive is a C# based parser for RDF originally held at www.drive.org, but at the time of writing the website has been removed.

Figure 12 below illustrates the interaction between the components.

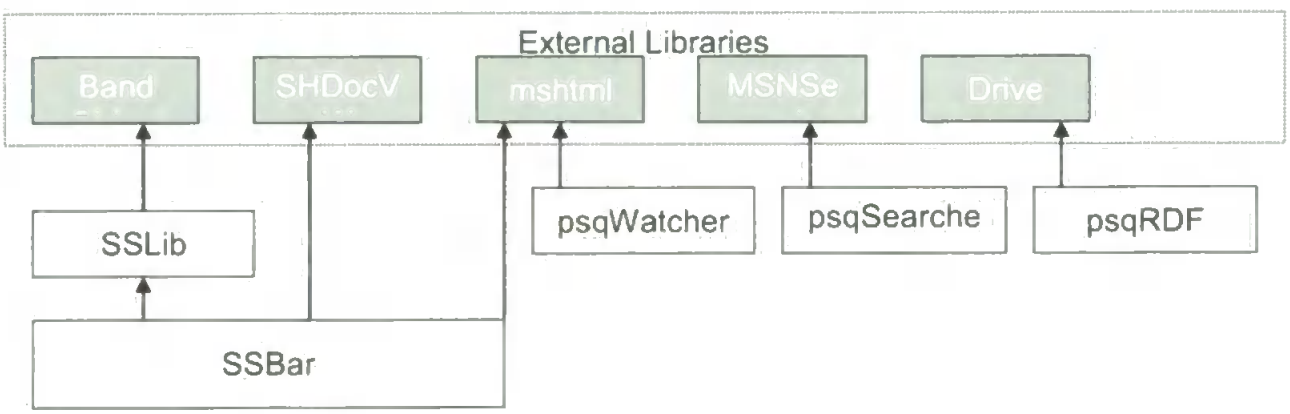


Figure 12: Interaction with external libraries

8.3 Interface

Implementation of the interface had to be mindful of the objective articulated in section 7.2 , that of being "simple and easy to understand". This objective reflects the basic tenets of

usability [Lauesen, 2005; Shneiderman & Plaisant, 2005], the primary relevant concepts to this research being:

- Being supportive of the tasks the user wishes to achieve;
- Easy to learn and hard to forget in a hurry;
- Easy to understand what the system is trying to achieve.

The interface was composed of four components: SSBar, psqGroup, psqAnalysis and vafSettings.

SSBar provides both the main entry to the protytype and provides the interface with the user through creating the toolbar within the Internet Explorer (IE) window. Careful consideration was given to the buttons on the toolbar in line with the usability requirements mentioned above. Icons were selected that provided a common metaphor for the user, for example, where there were warnings the simple traffic light approach was used to represent high (red), medium (yellow) and low (green) risk situations. One of the internal libraries, the psqReasoner described later in section 8.4 , controls the alerts to and from both the SSBar and the web page having been loaded into the browser. A colour scheme echoing the traffic light colour scheme is used to highlight entry fields on a webform that may cause concern, the difference being that low risk fields do not have green backgrounds as that might cause irritation.

Creating the SSBar project involved creating a Windows control lib project and inheriting from the SSLib band object mentioned earlier. The toolbar is illustrated below in Figure 13

and appears underneath the standard menu bar.

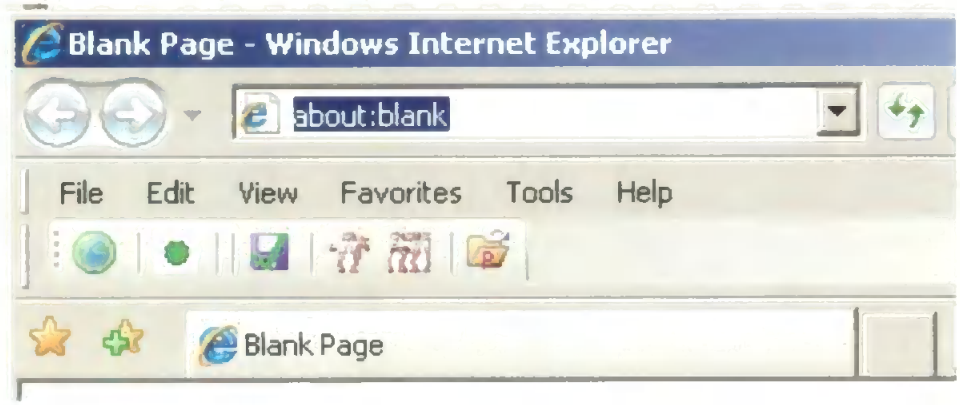


Figure 13: Toolbar Illustration

As described earlier, the SSBar component has external dependences on Interop.SHDocVW and Microsoft.mshtml external libraries. To ensure appropriate feedback from interactions with the rest of the libraries, delegate functions were utilised to create the callback functionality.

Figure 14 below illustrates the interaction between the interface components and the internal libraries.

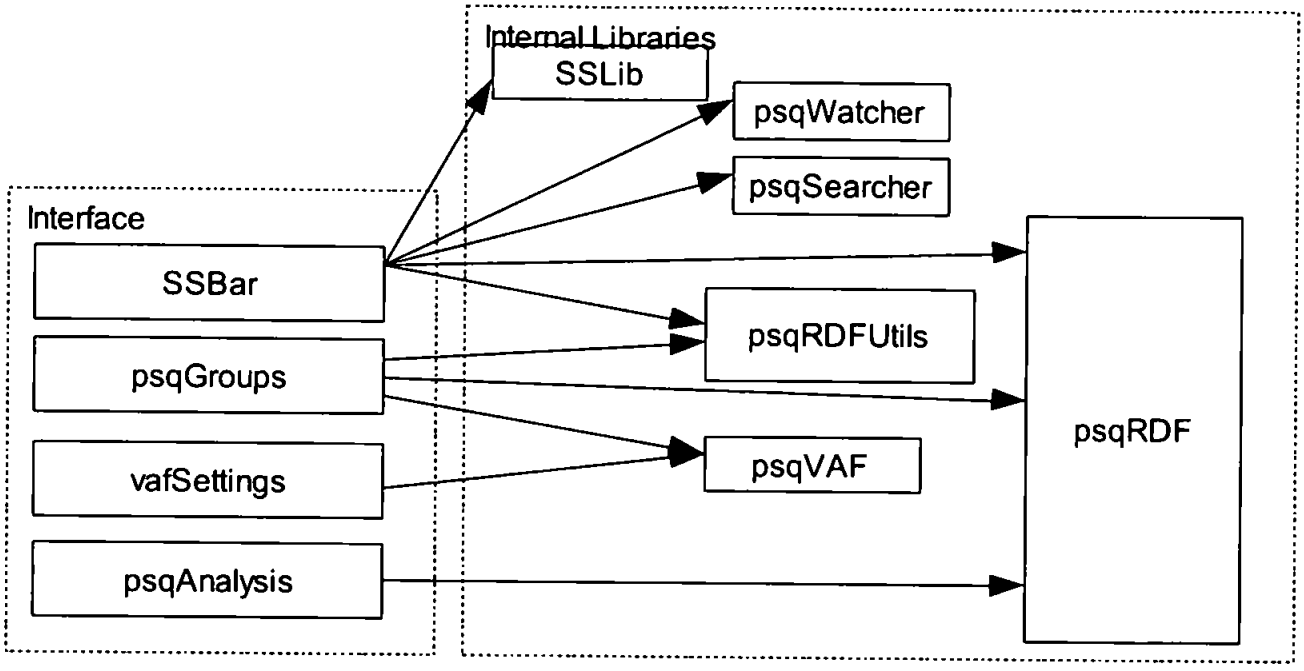


Figure 14: Interaction between interface and internal libraries

As SSBar loads, psqRDFUtils.doesFileExist is called to see if the user has previously entered their details. In a fully working prototype, this would be dependent upon a log-in for the individual to ensure that the correct person accessed the data. However, in this prototype this approach was not incorporated. If the data file is not found, the user is offered the opportunity of completing the settings and the vafSettings form is displayed. This form can also be accessed by selecting the single squirrel icon, the fourth icon along the toolbar from the left. The vafSettings form is dealt with in more detail later in this section. If the settings files are found, these are held in memory in RDF format by accessing the psqRDF component.

Once Internet Explorer has loaded and the user begins to interact with webpages, the internal library psqWatcher is instantiated. A callback function to change the display of the

circle illustrated in the second icon is passed to psqWatcher, this delegate function changes the status between green, yellow and red circle icons dependent upon the assessment made of the webpage. Different alert levels are associated with differing privacy levels according to the context of the user. That context is measured by the VAF rating.

The third icon along illustrates the recording status of the application and the icons were chosen to be as clear and explicit as possible. The purpose is to be explicit about the fact that information is being monitored, therefore a disk icon with a green tick was determined to be a useful indicator. Allowing the individual the ability to explicitly disable the monitoring tool, thus having explicit control over its usage, was considered an important element of the interface. The screenshot below, Figure 15, illustrates the icon showing when the collecting mechanism is turned off.

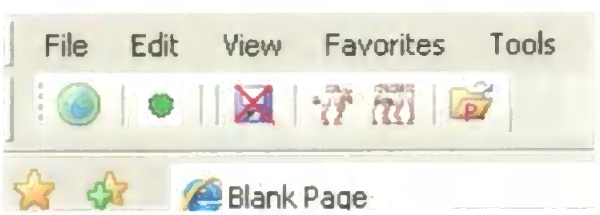


Figure 15: No Save Icon

psqAnalysis, psqGroups and vafSettings are windows forms providing the interface for the user to interact with the prototype and have been designed so that relevant information is grouped together. psqAnalysis is accessed by selecting the folder icon showing P at the far end of the SSBar. This windows form is passed two RDF documents held in memory in psqRDF classes along with two callback functions to provide the facility to navigate to a

specific URL and to write the RDF document. The graphics are created based upon the numbers contained in the RDF files and are shown below in Figure 14.

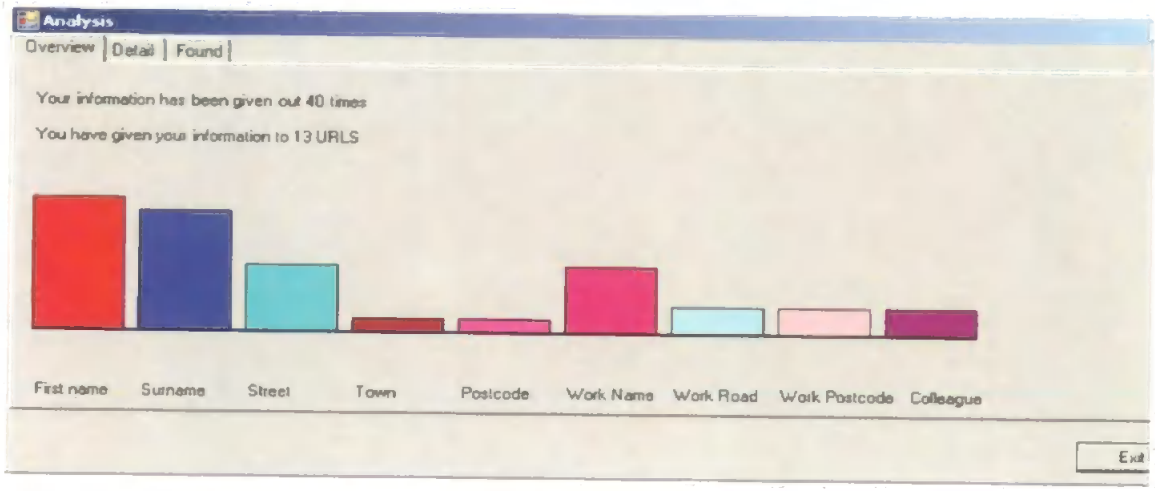


Figure 16: Analysis Page

This analysis page illustrates a simple bar chart designed to present an overview of the amount of information divulged. This includes the number of times information has been given out along with the number of distinct URLs. Each category of information is represented in the form of a bar, starting with name, through address to work and work colleagues. The bar chart analogy was chosen as an easily understood format that can provide a visual representation of the amount of information given out.

The second page illustrates where the information has been given out and is shown below in Figure 17. The tree view component was used here to give control to the user over how much information was displayed, allowing for the user to drill down into the entries that are of particular interest, rather than displaying too much information in one screen. This gives the item of information that has been divulged, along with the URL where it has been given

out. On a right click the user can navigate to the page where the information was given.

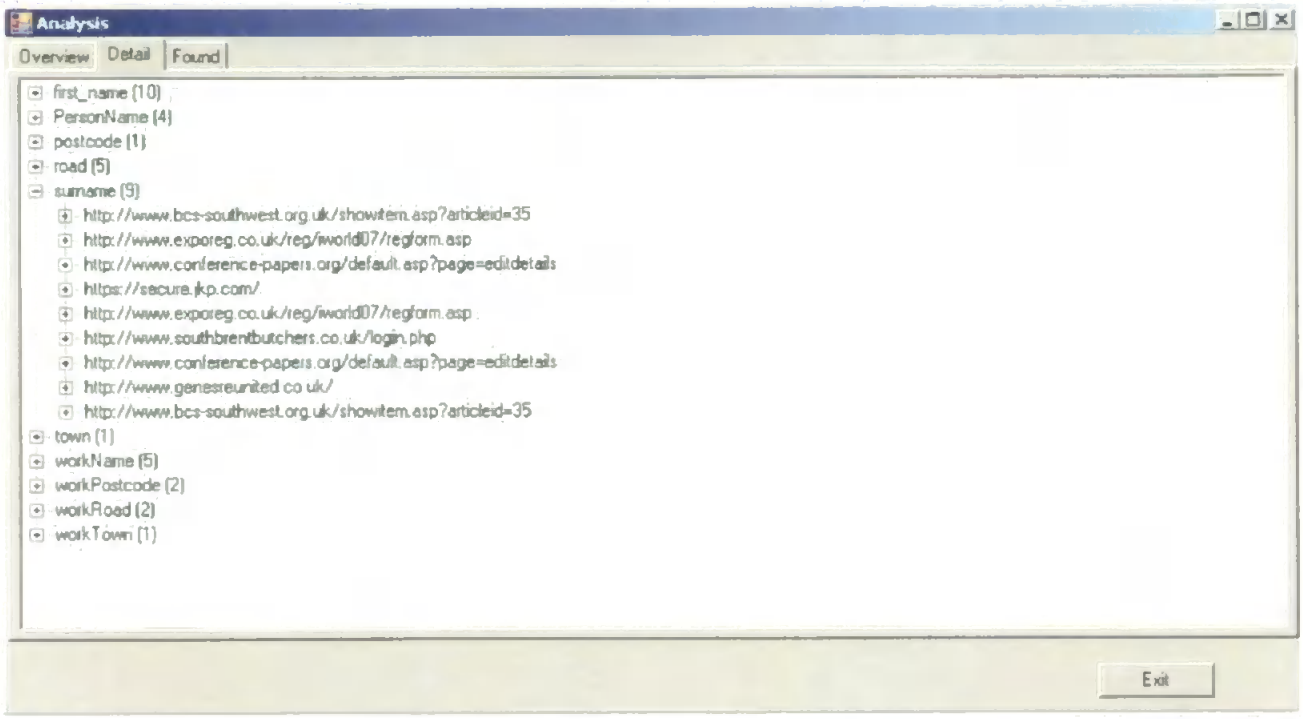


Figure 17: : Detail where personal information divulged

The final page on this form, gives the details of where information has been found. This also allows the user to navigate to the URL. This is illustrated below in Figure 18.

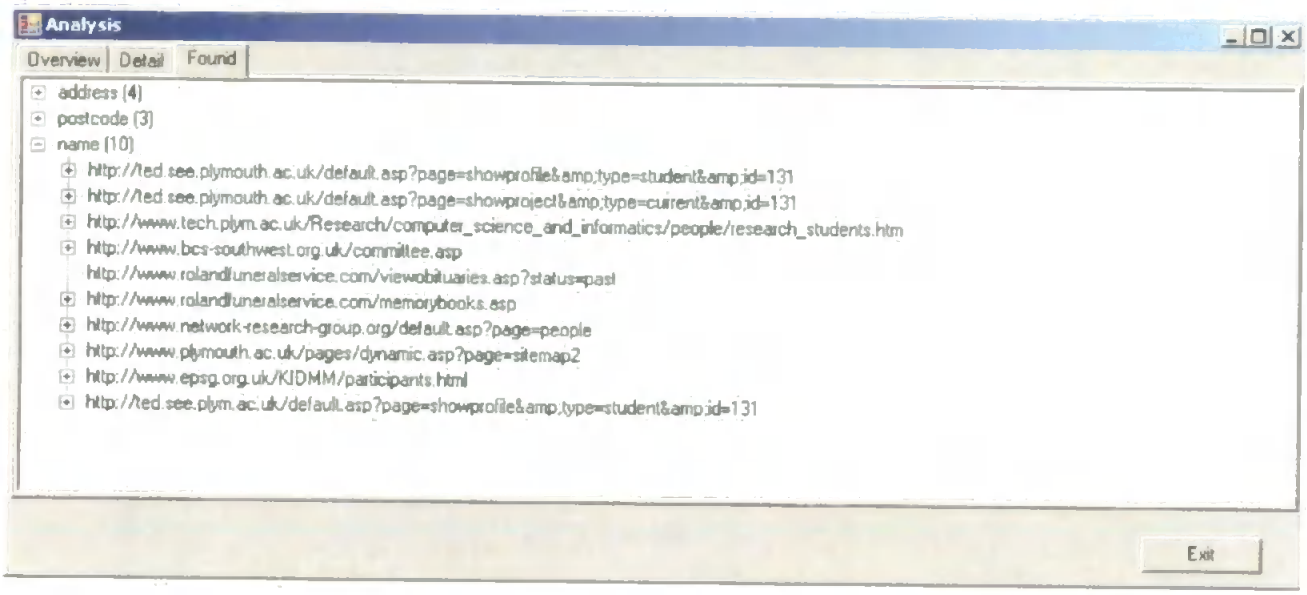


Figure 18: Where personal data found

The vafSettings form is either displayed on first use if the user agrees, or can be selected from the single squirrel icon. On loading, this form accesses the psqVAF internal library which loads in existing information from a file if appropriate. If there is pre-existing information, this is displayed to the user. This form demonstrates the implementation of the VAF as discussed in section 7.3.1 , and poses two pages of questions to the user. The questions demonstrated for this prototype are fairly limited examples of the type of questions that could be posed and are mentioned as one of the areas where further work will be required in section 10.3 . The first page collects static factor information which concerns things that do not change very often. In this example, gender, name and address, both home and work are used. The second page covers more dynamic factors, and includes questions on usage and a self-assessment of technology capability, roughly divided into three categories. Figure 19 illustrates the two separate pages on the settings

form.

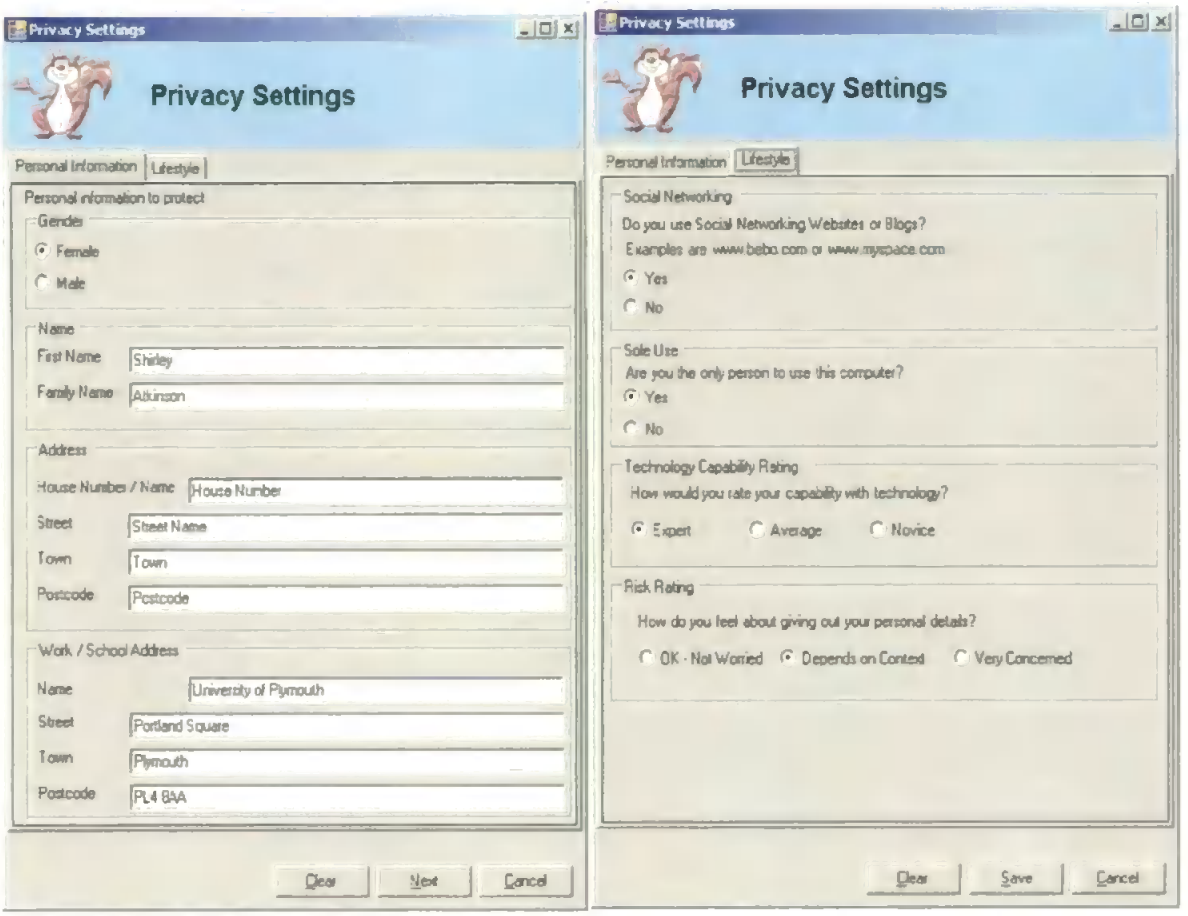


Figure 19: Privacy Settings Entry Pages

As the user exits the form, the answers from these questions are saved to a file on the hard drive in RDF format and weightings for personal information devised from the answers. The weightings are expressed in three levels as initially determined in the discussion about the VAF settings in section Vulnerability Assessment Framework. This will be discussed in more detail in section 8.4 Internal Libraries when discussing the psqVAF component and in section 8.5 when discussing the data files. Following the user saving and the vafSettings form closing, the psqSearcher component is accessed to begin a search for personal information publicly displayed based upon the data collected.

The psqGroup component is accessed through the icon containing the group of squirrels. This presents a form to the user to enter information about the organisation and the individuals within that organisation who might require monitoring. These are saved in the same fashion as the information collected from the vafSettings form. The data is saved within the existing RDF settings and are utilised by the psqVAF component when monitoring the individuals' interactions with the webpage.

8.4 Internal Libraries

The internal libraries psqRDF, psqRDFUtils, psqWatcher, psqReasoner, psqSearcher and psqVAF are each described in turn below. A class diagram representing their interactions is given in Figure 20.

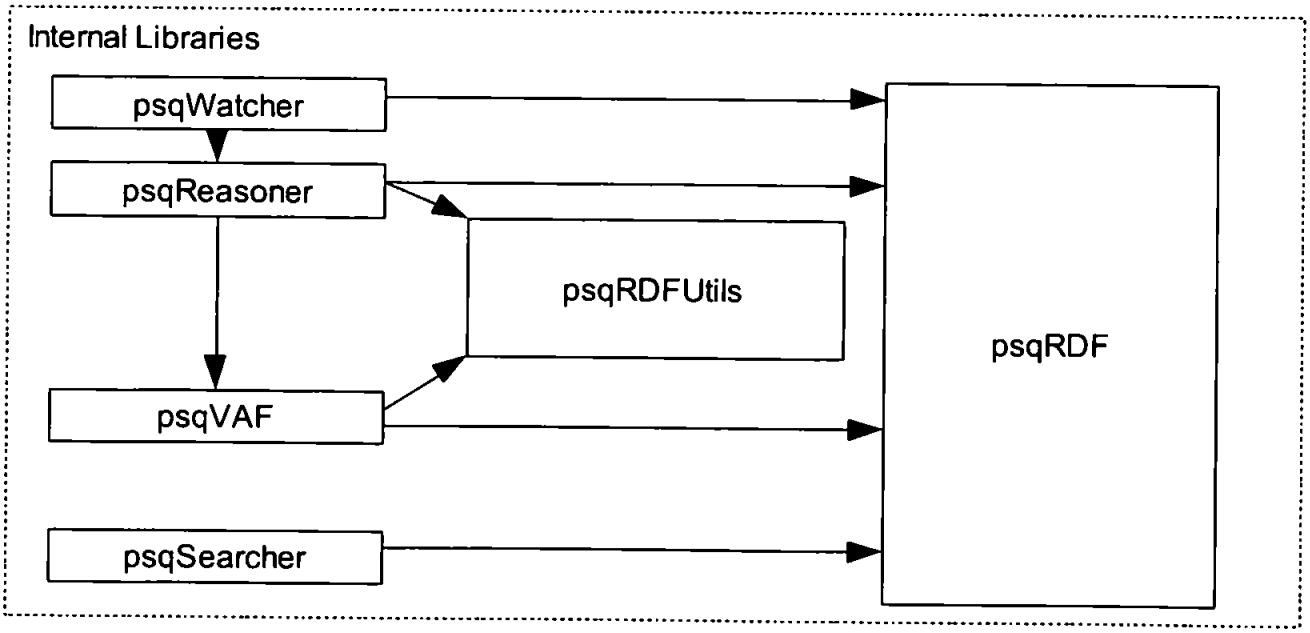


Figure 20: Internal Libraries

The psqRDF is a key component within the system. This interacts with the external library Drive.dll to provide the core functionality for manipulating RDF structures. The component is called either to create a new empty RDF graph for adding data to or is passed in a URL for creating an RDF graph in memory from that file. This URL can represent either a file held on the local machine or a URL accessed through the normal http protocols. The RDF graph is a collection of nodes containing triples that can be searched through, and methods are provided that search these triples for specific subjects, objects or predicates. Due to the lack of facility within the Drive.dll to write RDF files, this component returns a string containing the XML description of the RDF file, built from the triples contained in the RDF graph in memory. This component does not access any other component but is utilised throughout the prototype for holding the data.

The psqRDFUtils component provides the functionality to check if a file exists. There are also methods to load data into the psqRDF component and save the RDF files to the hard drive. The components SSBar, psqVAF, psqGroups and the psqReasoner interact with this component.

The psqWatcher component is another core component and is initiated by the SSBar the interface when a web page is loaded. Passed into the constructor are data settings in RDF format, a reference to the HTML page loaded into the browser and six delegate functions each concerning a specific element of display. Once the page is loaded, the RDF data is queried to ascertain if there is already any privacy information held within the existing data store. This allows for an approach which could be extended should the Semantic Web become more commonplace. The web page links are examined to

determine if there are any associated RDF files or P3P files. Links are HTML elements already in use by web pages to associate certain files and would appear a logical approach for associating RDF and P3P. However, at the time of writing, linking these types of files is not a common standard initiated by the W3C, nor a common approach for many web developers to utilise. Therefore, whilst the functionality was put into place to demonstrate how this might work if it were commonplace, this was not the primary approach to be adopted by the prototype. The purpose of any associated RDF files would be to describe the data held within the web page itself, the P3P files would describe any associated privacy policies, P3P being an agreed W3C format for expressing privacy policies. Therefore, if there was to be a common ontology for describing the collection of personal data, this would allow for more fine grained reasoning to be carried out. The next step is where the psqReasoner is called to examine the input fields on the page. If there are input fields, an event handler is added to the relevant button. Input fields have their background colour altered depending upon the rating allocated by the reasoner, for example a postcode has a high risk rating and a field on a web form collecting this information would be highlighted in red. The event handler works on the mouse down, primarily because it is not possible to chain the onClick events of the HTML button element. In the event of the button being clicked, all input fields on the web page are assessed to determine if the data they are submitting matches the personal data held in the settings. If there is a match, the information about the URL, type of data and date are recorded using the delegate callback function.

The psqReasoner component is passed information by the watcher for evaluation. On instantiation, the psqReasoner holds a callback function in order to communicate the

privacy status. This takes the format of an enumerator providing the values OK, ALERT and WARN which exactly correlate to the VAF rating as described in section 7.3.1 . The psqReasoner uses a simple string matching process to determine whether the input element names are contained in the VAF ontology. The psqVAF component is utilised to return the risk rating for the individual elements. In addition to processing any of the input field values to determine if they contain information that should be monitored, in the event of there being any associated RDF files, these are queried to determine if they are collecting information.

Searching is performed by the psqSearcher component when called by the SSBar interface, either called explicitly by the user or initiated on first completion of the privacy settings. This interacts with the MSN webservice to obtain search results for name, address and postcode. When the routine is finished, a callback function is utilised to save the information in RDF format.

The psqVAF component provides the functionality to interface with the Vulnerability Assessment Framework. Settings pertinent to the individual are loaded into memory from a file in RDF format. Data collected is added to the RDF file and psqRDFUtils is accessed to write this data to the hard drive. This component also provides the item ratings, informing the reasoner what rating the piece of information has been allocated within the VAF ontology. An overall risk rating value is also calculated by adding together the values from the answers given to the vafSettings questions. The snippet of code below illustrates the routine in the psqVAF that determines what icon should be shown.

```
private psqStat getStatusLevel()

    {
       psqStat pReturn = psqStat.psq_ALERT;  //Yellow circle
       if (pVAF.iVAFScore < 15)
          pReturn = psqStat.psq_ALERT;  //Yellow circle
       if (pVAF.iVAFScore > 15)
          pReturn = psqStat.psq_WARN;  //Red circle
       return pReturn;
    }
```

This routine illustrates that if the overall VAF rating is over 15 this denotes an individual likely to be in a high risk category and therefore requires that the icon should display a red circle.

8.5 Data files

As described in the sections above, XML files storing RDF formatted information form the basis for the data storage in this prototype. There are five files in use: vaf.xml, currentsettings.xml, groupsettings.xml, found.xml, and visited.xml. These all conform to the same standard for holding information, and are stored in the same folder.

The VAF ontology file is the only one not held on the users machine but held in a central location. The ontology is expressed in the OWL format, an established protocol as discussed in section 7.4.1 , with the purpose of outlining which personal data elements were considered important for protection. An additional brief ontology, Pif, was created for describing web pages that collect personal information. This was for use as a potential method for inserting RDF statements into web pages to describe whether the web page had a privacy policy, or the page in general was collecting personal information. .

Fragments of the main VAF ontology are explained below, and the full document can be found on the accompanying CD-ROM.

```
<?xml version="1.0"?>
<rdf:RDF xmlns:dc="http://purl.org/dc/elements/1.1/"
xmlns:foaf="http://xmlns.com/foaf/0.1/" xmlns:owl="http://www.w3.org/2002/07/owl#"
xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#" xmlns:vaf="http://www.shirleyatkinson.com/ontology/vaf#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema#">
```

The ontology refers to an existing ontology, the Friend of a Friend (FOAF). This already refers to information about individuals and illustrates how ontologies are being combined.

```
<owl:Ontology rdf:about="http://www.shirleyatkinson.com/ontologies/vaf">
<rdfs:comment>Ontology to describe the vulnerability assessment framework. Gives ratings to personal information</rdfs:comment>
<rdfs:label>Vulnerability Assessment Ontology</rdfs:label>
<dc:title>An Owl ontology to describe the personal data elements, risk element and rating for the protection to be given to personal information</dc:title>
<dc:description>This ontology model describes the ratings and data elements that people wish to protect with regard to personal information</dc:description>
```

This part of the document gives the information about the purpose of the ontology. The namespace dc illustrates the use of the dublin core format for expressing information about the document.

```
<owl:Class rdf:about="http://www.shirleyatkinson.com/ontology/vaf#PersonalData" rdfs:comment="A person.">
<rdfs:subClassOf rdf:resource="http://xmlns.com/foaf/0.1/Person"/>
<rdfs:label>Person</rdfs:label>
</owl:Class>
        <owl:ObjectProperty
rdf:about="http://www.shirleyatkinson.com/ontology/vaf#protectionRating" rdfs:comment="Defines the protection rating that people wish to give to their personal data" rdfs:label="Protection Rating">
<rdfs:domain  rdf:resource="http://www.shirleyatkinson.com/ontology/vaf#PersonalData"/>
<rdfs:subPropertyOf rdf:resource="http://www.shirleyatkinson.com/ontology/vaf#family_name"/>
<rdfs:subPropertyOf rdf:resource="http://www.shirleyatkinson.com/ontology/vaf#firstName"/>
<rdfs:subPropertyOf rdf:resource="http://www.shirleyatkinson.com/ontology/vaf#gender"/>
<rdfs:subPropertyOf rdf:resource="http://www.shirleyatkinson.com/ontology/vaf#hNum"/>
<rdfs:subPropertyOf rdf:resource="http://www.shirleyatkinson.com/ontology/vaf#road"/>
<rdfs:subPropertyOf rdf:resource="http://www.shirleyatkinson.com/ontology/vaf#town"/>
<rdfs:subPropertyOf rdf:resource="http://www.shirleyatkinson.com/ontology/vaf#pCode"/>
<rdfs:subPropertyOf rdf:resource="http://www.shirleyatkinson.com/ontology/vaf#birthday"/>
</owl:ObjectProperty>
```

This fragment outlines each of the specific elements of personal data and relates to the specific ratings being in the VAF settings file.

Utilising the VAF ontology allows the PSQ to create a settings file, vaf.xml. This allocates the ratings on the individual elements of information. An example is given below showing the elements birthday, road and postcode and their respective protection ratings.

```
<rdf:Description rdf:about="http://www.shirleyatkinson.com/ontology/vaf#birthday">
        <vaf:protectionRating>2</vaf:protectionRating>
</rdf:Description>

<rdf:Description rdf:about="http://www.shirleyatkinson.com/ontology/vaf#road">
        <vaf:protectionRating>1</vaf:protectionRating>
</rdf:Description>

<rdf:Description rdf:about="http://www.shirleyatkinson.com/ontology/vaf#postcode">
        <vaf:protectionRating>2</vaf:protectionRating>
</rdf:Description>
```

The following fragment of RDF is taken from the current settings XML file and illustrates the format information stored about the individual. The element Person has a first name, family name, gender, work name, work road, work town, work postcode. In this fragment the VAF rating is illustrated for the work road and the gender.

```
<rdf:Description  rdf:about="http://www.shirleyatkinson.com/ontology/vaf#Person">
<vaf:first_name>Shirley</vaf:first_name>
<vaf:family_name>Atkinson</vaf:family_name>
<vaf:gender>Female</vaf:gender>
<vaf:workName>University of Plymouth</vaf:workName>
<vaf:workRoad>Portland Square</vaf:workRoad>
<vaf:workTown>Plymouth</vaf:workTown>
<vaf:workPostcode>PL4 8AA</vaf:workPostcode>
</rdf:Description>

<rdf:Description  rdf:about="http://www.shirleyatkinson.com/ontology/vaf#workRoad">
<vaf:hasRating>1</vaf:hasRating> </rdf:Description>

<rdf:Description  rdf:about="http://www.shirleyatkinson.com/ontology/vaf#gender">
<vaf:hasRating>0</vaf:hasRating> </rdf:Description>
```

8.6 Demonstration

The PSQ interface was carefully designed to address some of the criticisms already levelled at existing PETs, as discussed in section 3.4 , in addition to addressing the context within which the respondents found themselves. It was required to be part of the

everyday tools utilised by the individual; to provide enough information to be useful, exerting enough cognitive friction to make the individual aware of what they were doing, but not too much of a cognitive overload that they would begin to ignore the alerts; and to provide the wherewithal for the individual to be able to exert control over their personal information.

To recap, the prototype had four primary objectives which were:

- to provide an environment which would facilitate individuals linking their actions to the consequences of their actions;
- to encourage the individual to be proactive in controlling the flow of their personal information by providing an environment where they could monitor where their personal information was being given out;
- to provide a simple and easy to understand interface;
- to not require explicit choice of protection.

The prototype analyses the web pages unobtrusively in the background, highlighting fields collecting personal information when necessary. The screenshot in Figure 21 below gives an indication of how PSQ will alert the user should they need to be wary of giving out their personal information.

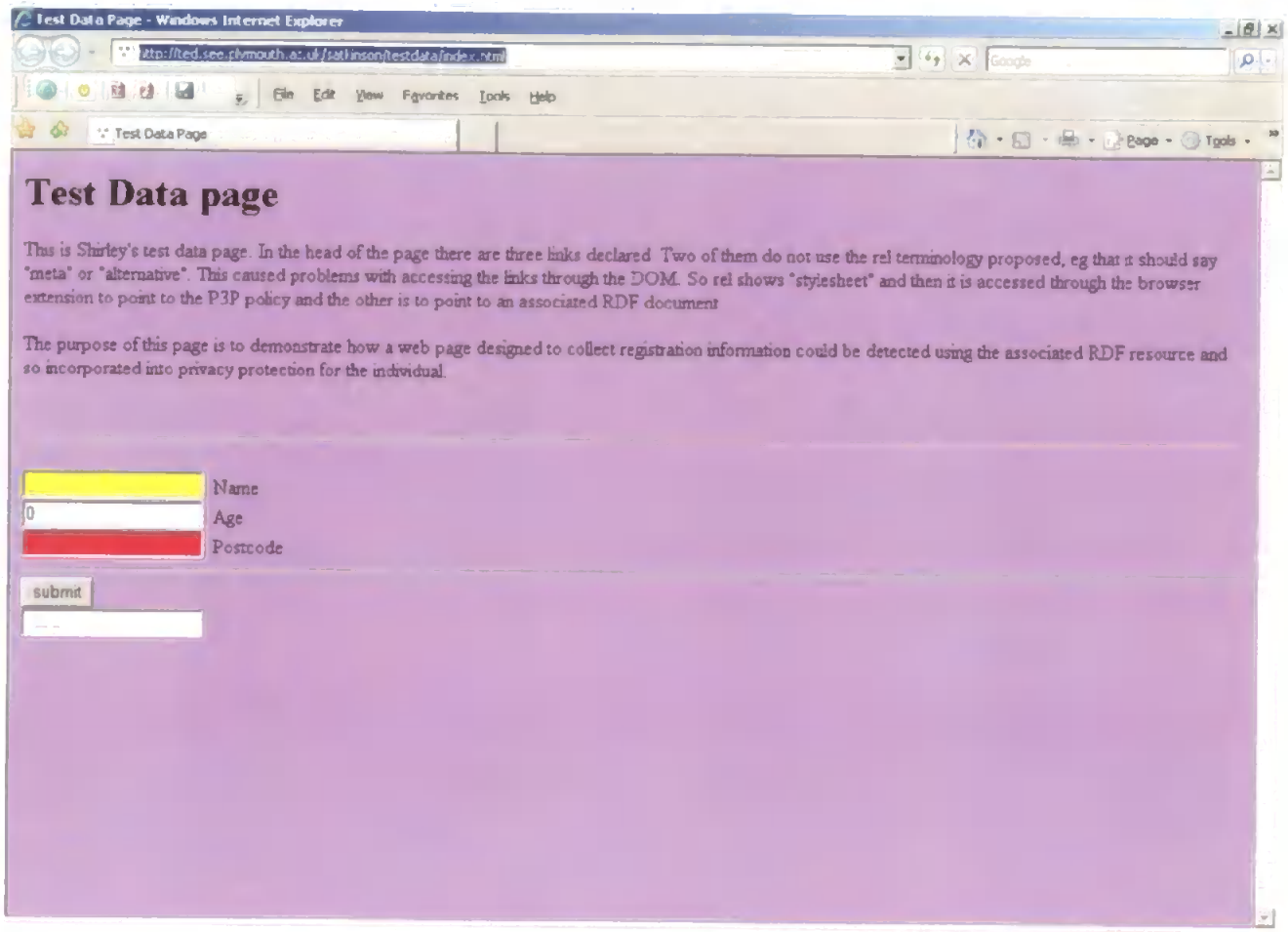


Figure 21: Test data page

Along the toolbar, the circle icon is showing yellow to illustrate that there is some concern surrounding what information this page is collecting. The icons alongside illustrate that there is an RDF file and an associated P3P file which can be utilised by PSQ to reason with using Semantic Web techniques, as and when they evolve. Moving to the page itself, PSQ has highlighted two of the input fields. The first field, Name, is deemed to warrant a yellow highlight, whereas the Postcode field warrants the red highlight - given that it has a higher risk rating than name. The levels are determined from the VAF settings and can easily be changed depending upon the context of the user.

The screenshot in Figure 22 illustrates a page that is not collecting personal information.

Along the toolbar the circle icon is green and the search input field is not highlighted.

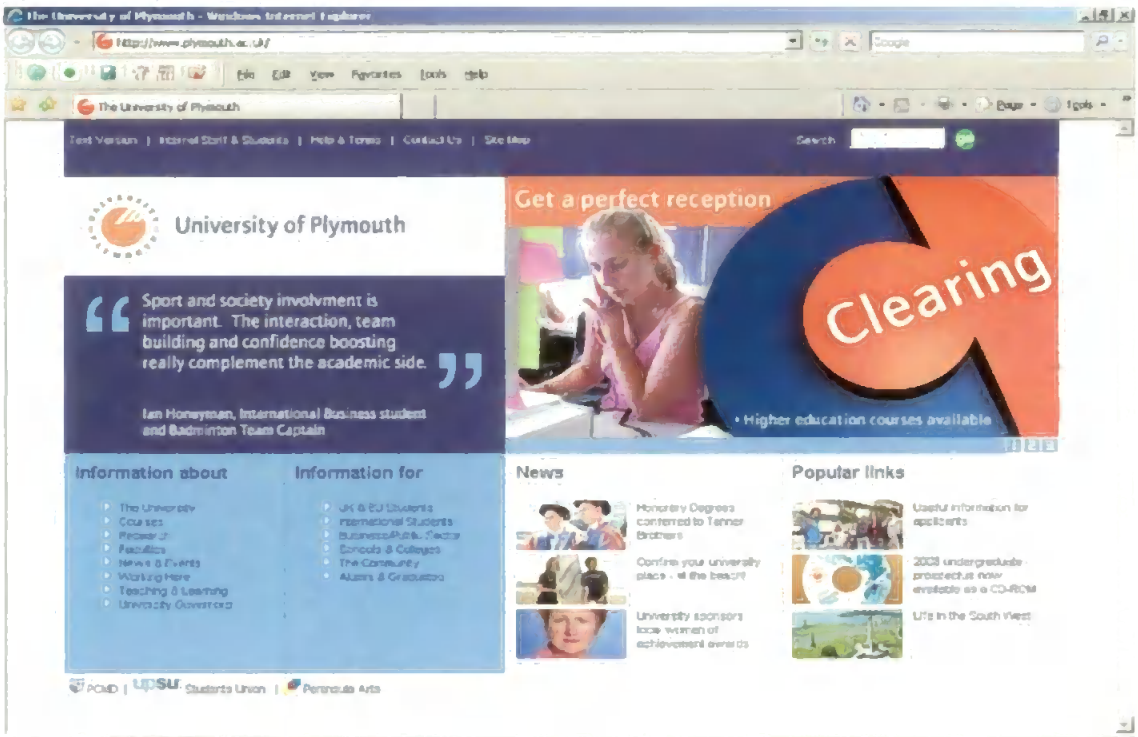


Figure 22: Webpage

8.7 Conclusion

This chapter has outlined in more detail how the main features of the conceptual architecture have been implemented to allow the user more control over their personal information. The monitoring and recording facilities allowing the user control over the actions they take, along with the customisation and tailoring of the alerts to the context of the individual, were also demonstrated through the use and understanding of different risk factors as demonstrated through the use of the VAF. Rules were represented in RDF, allowing for reasoning and the use of the ontology demonstrated how the PSQ could be

extended at a later date should Semantic Web techniques evolve further and become more common place.

The development of the prototype has helped to realise how useful the Semantic Web approach can be, allowing for flexibility in reasoning and the ability to add further components without rebuilding the software. PSQ also demonstrated how the conceptual architecture could be implemented, thus adding to the proving of its' viability. The prototype allows for a more practical validation of the ability to achieve a privacy enhancing technology that is tailored to the context of the respondents involved in this research. Therefore, the system offers a direction for PETs, an advancement of existing approaches that factors in more detailed understanding of the social factors influencing the risks to individuals. The next stage however, is to explore in more depth how individuals are likely to react to this software and so involves the respondents in an evaluation exercise. This evaluation is presented in the following chapter.

9 Exploratory Prototype Evaluation

This chapter begins with a recap of the original objectives for the research, outlining how the prototype aimed to demonstrate these objectives. A discussion follows concerning the methods utilised to carry out the evaluation. The findings are introduced and two test scenarios are considered to further illustrate how the prototype acts as a tool for risk reduction. The chapter concludes by considering what the findings demonstrate about the prototype.

9.1 Introduction

> "*innovation starts with people... if you forget this even for a moment, you run the risk of delivering feature-rich rubbish into already overcrowded lives*" [Seymour, 2002]

As Seymour outlines above, it was important that representatives from the user populations provided a central element to the evaluation process. Involving respondents in such a fashion is an already established and important aspect for both user-centred [Wagner, 2005] and participatory design [Bakardjieva, 2005]. The prototype was a technological tool created by the author for addressing the problems of vulnerability and set out to explore the primary hypothesis outlined in section 4.3 , the hypothesis being that the less personal information is divulged, the less of a risk is posed to the individual. To address this essentially subjective approach, representatives of the user populations were invited to provide their opinion on the usefulness of the prototype.

It is worth mentioning here the Technology Acceptance Model (TAM) [Davis et al, 1989]. This was proposed as a way of assessing user acceptance of software and comprises perceived usefulness and perceived ease of use. At first glance it would appear to be

relevant to the evaluation of this prototype, seeking user opinion on how useful the features of the prototype would be. This model was not considered to be entirely appropriate for this exploratory evaluation of the prototype for the following reasons. TAM could be seen as useful if this research was being conducted in a software-centric fashion. However, the prototype software here was not being developed as a full working application and therefore did not suit that context. The purpose of the prototype was to demonstrate a potential approach towards risk management, and it was therefore the focus of the potential for limiting risks to individuals that was the focus of the evaluation.

To learn from the opinions of the respondents, the evaluation phase set out to measure their attitude towards the PSQ prototype. The evaluation hypothesis was that:

> *The more favourable the attitude, the more likely it is that the software will be used. Individuals are therefore more likely to exert control over their own personal information which will in turn reduce their vulnerability.*

The hypothesis above is built from assumptions based upon the literature and has been composed as follows.

> *The more favourable the attitude, the more likely it is that the software will be used.*

A positive attitude from the users of any software is considered a basic requirement for that software to have a successful implementation [Gallivan and Keil, 2003; Heath and Luff, 2000].

> *Individuals are therefore more likely to exert control over their own personal information*

The behaviour of an individual is often influenced by their perception of their environment [Suchmann, 1991; Hine, 2000]. More in-depth discussion relating to these concepts were

introduced in sections 3.3 and 6.3 . Both Cavoukian and Tapscott [1997] and Feenberg [1999] consider how individuals alter their behaviour when under observation.

which will in turn reduce their vulnerability.

This refers explicitly to the findings from both Dinev and Hart [2004] and Margulis [1977] who found a direct correlation between release of personal information and the concepts of vulnerability. As discussed in section 4.3 , vulnerability was considered in terms of the effects that privacy breaches had on individuals.

9.2 Objectives

The second phase of the research set out to utilise technology to mitigate the risks arising from the potential abuse of personal information. The conceptual architecture design for the PSQ prototype set out to influence the behaviour of the individual so that the amount of personal information given out was both reduced and controlled. Restrictive measures have been found to be unpopular [Livingstone and Bober, 2005], and the advice given by government campaigns to control and protect personal information has either not been seen as relevant, or the advice has not been received [Lacohee et al, 2006]. The respondents attitude towards the PSQ prototype was therefore considered a useful indicator to determine whether the risk reduction approach could be delivered in such a way that was not either unpopular, condescending, or restrictive.

To recap, the objectives for the prototype were as follows:

- to demonstrate the conceptual architecture;

- to offer assistance to the individual to control personal information;
- to provide an environment that would facilitate the ability to link actions to consequences;
- to allow the individual to proactively control the flow of personal information from themselves by providing an environment that monitored where personal information is given out;
- to make the privacy tool as simple and easy to understand as possible;
- to provide a privacy tool that did not require an explicit choice of protection.

9.3 Evaluation Method

The evaluation was an exploratory foray into how a privacy supportive piece of software might operate and as such were brief in nature. Participants did not use the software themselves, but were shown the key features as described in section 7.3 on functionality. These demonstrations were to be the first steps in the evaluation process, allowing for findings to inform and influence the development of the prototype. Further refinement and user involvement could follow if the indications were positive. As such, there were no control groups and no measures of the effect of the demonstrator upon the participants, factors that would need to be addressed with further work.

The evaluation phase sought to combine an overall qualitative approach with an element of quantitative analysis. The early stages of the research as introduced in section 4.3 relied upon gathering respondents attitudes and beliefs without the constraints of a fixed agenda, but this free-form approach was not suitable for answering the specific questions

required for evaluation. Respondents were again invited to participate in focus groups, semi-structured interviews and an online survey.

The format for both focus groups and interviews were the same, where the researcher gave a demonstration of the PSQ prototype software, and respondents were asked to complete a questionnaire. The opportunity for discussion was also provided.

The questionnaire was the vehicle to measure the respondents' attitude towards the software and provided the data for the quantitative analysis. Statements were made about specific elements of the PSQ prototype that correlated to the requirements, answers were constrained by a Likert scale and spaces were allowed for comments. A 5-point Likert scale was utilised with 1 indicating the feature was not very helpful and 5 indicating the feature was very helpful. The respondents were left to choose their own value of "helpfulness" from the numbers between 1 and 5 rather than having terms to describe the measure in the anticipation that terms would influence their choices.

A criticism of using focus groups for software evaluation was made by Cooper [2004], who stated that the participants were likely to be ignorant of what the software can and cannot do, and potentially could make requests for features based upon a short-sighted perspective. The questionnaire used in these focus groups was therefore designed in part to address this potential failing. The statements within the questionnaire were carefully chosen to direct attention to the requirements of the prototype and the Likert

scale responses chosen to give some structure to the answers. The Likert scale has been described by Bryman [2004] as being one of the most common approaches to investigating attitudes towards specific concepts, and it has also been identified as one of the most popular question formats for assessing usability [Dumas, 1999]. The full approach advocated by Likert whereby the list of statements are piloted and refined prior to launching upon a wider audience was not utilised here due to time constraints [Kent, 2001].

Allocating numbers to a scale of attitude can bring about the criticism that this is attempting to measure a concept that does not inherently possess a numerical scale, and therefore is being constrained by imposing numerical values upon it. However, it is useful as an overall guide providing that these numbers are not considered to provide absolute values. Likewise, the Likert scale attracts criticism both in relation to lack of validity and the ability to be reproduced. Therefore the scale was used only to give guideline rankings and to provide further exploration of each element of the respondents' feelings towards the prototype. Respondents answers could only be used as reflections of their feelings towards the prototype at that moment in time, rather than as a specific generalisable measure.

Difficulties were encountered in including the same participants as before, due to many having left the school following their examinations. Two of the community based focus groups did engage with the same young people as before. Five focus groups were held in total with a total number of thirty-three young people between the ages of thirteen and

nineteen. The opinions of those with responsibility for the safety of young people were also sought through a selection of parents and teachers. Semi-structured interviews were held with representatives from CEOP, along with managers from Women's Aid refuges. Workshops at the Women's Aid national conference again facilitated interaction with front line staff. The opinions of individuals, some of whom had participated in the original interviews, were collected through the use of an online questionnaire. During each of the focus groups or interviews, the researcher outlined each of the pertinent elements of the PSQ prototype, allowing time for the respondents to answer questions and to complete the questionnaire. In addition to the ranking, opportunities were given for the respondents to discuss and comment upon the statements and the prototype in general.

To further explore how the prototype would assist the individual in controlling their personal information, two theoretical scenarios were explored and are presented in section 9.5. The purpose of using the scenarios was to explore in greater depth exactly how the prototype would perform and to assess the suitability of the prototype.

9.4 Findings

9.4.1 Overview

Of those respondents who completed the questionnaire, forty-five responses were collected in total with thirty-three of those responses coming from young people between the ages of thirteen and nineteen. The following table illustrates the overall descriptive statistics of minimum, maximum, median and skew values.

	Overall	*Age < 20*	*Age => 20*
Min	1	1	1
Max	5	5	5
Median	4	4	4
Skew	-0.7	-0.8	-0.22

Table 13: Descriptive statistics for entire data

The histograms in Figure 23 illustrate the values given for the overall and pertinent age categories as an overview of how helpful the prototype was considered to be.

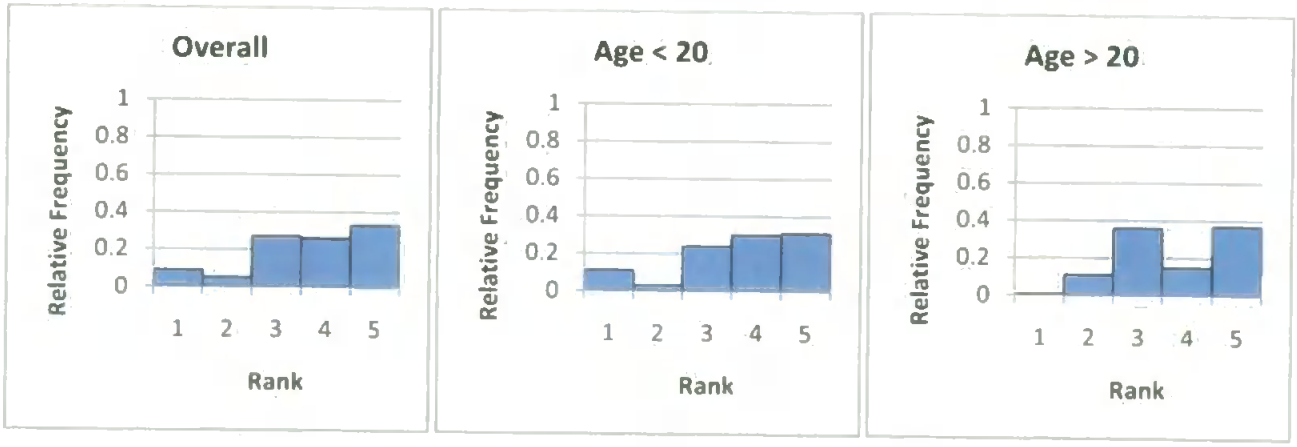


Figure 23: Overall Categories

59% of the respondents gave positive ratings for the software, giving a ranking of over three. Indeed 33% of the respondents awarded the prototype a rating of five to indicate they thought it would be very helpful, compared to 9% who felt it was not helpful at all. In this example, the data is not symmetric and therefore the measure of either the mean or standard deviation would not be correct, the overall category carried a skew measure of -0.7. The median measure therefore gives a more effective and robust illustration. In this

instance, the median value is four and serves to illustrate a reported positive attitude held by the respondents towards the prototype. These figures however are viewed with an understanding that the tendency for individuals to report positively on their feelings is likely to be a contributory factor.

The overall figures were further analysed using two age categories. Those of the under twenty year olds to represent the teenage respondents and those considered to be aged twenty years old and over, the adult respondents. Conducting a more fine grained analysis of the age groupings was not considered necessary and so details of the exact ages of the respondents were not collected.

By analysing the findings from both the age groups, it can be seen that the adults data does not have such a high skew value, the skew value being -0.22. The minimum, maximum and median values for both age groups are the same and so do not represent any variation because of age. However, by examining the relative frequencies of the overall rankings of four and five, it can be seen that more teenage respondents, 61%, valued the prototype more highly than the adults, 53%. Of those, 31% of teenage respondents and 37% of adult respondents gave the highest rating available. A large variation is seen in the allocation of the lowest rating of one, 11% of teenagers compared to 0.01% of adults. The highest ranking of the adults responses shows itself as being the middle ground, which can be an indicator of a number of things. It is possible that the adults were reluctant to commit themselves to a value, or that because the adults involved in the discussions were responsible for the safety of others, they were much more risk

averse and less likely to commit to an opinion. However, the statistics gleaned from the respondents indicate a predominantly favourable attitude towards the prototype.

The discussions surrounding the prototype in general, rather than specifically about elements within it, considered where the control of the information was to be held. Teenage respondents were concerned about whether they could password protect the information so that parents could not access it. Respondents who held a duty of care for other individuals considered it to be important that the organisation had access to the data rather than just the users of the software. In both refuge and school situations, it was perceived that a condition of use of the Internet would be to use the software for monitoring personal information.

9.4.2 Prototype features

Figure 22 illustrates the rank order in which the features of the prototype emerged. Whilst the exercise was not for the respondents to give these features a ranking, the ranking is used to provide an order for discussion, not to deem any specific value.

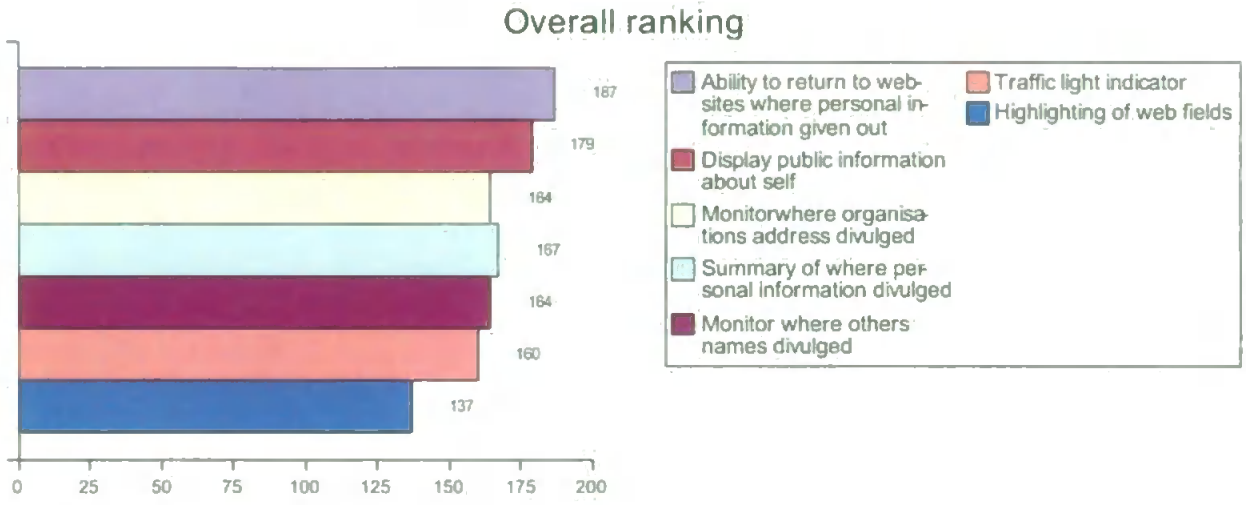


Figure 22: Overall Ranking

Each of the elements are discussed in turn by first introducing the data collected, giving the basic descriptive statistics of minimum, maximum, median and skew in categories relating to overall values, the teenage respondents values (age < 20) and the adults (age =>20). As with the overall statistics, the median values are considered to account for the skewing of the data. The three categories are illustrated by separate histograms so that the differences between the three categories can be more easily discerned. Discussions on each element followed the comments regarding the descriptive statistics.

Ability to visit webpages where personal information given out.

	Overall	***Age < 20***	***Age => 20***
Min	1	1	1
Max	5	5	5
Median	5	5	3
Skew	-1.52	-2.24	-0.44

Table 14: Breakdown of figures for Ability to return to website

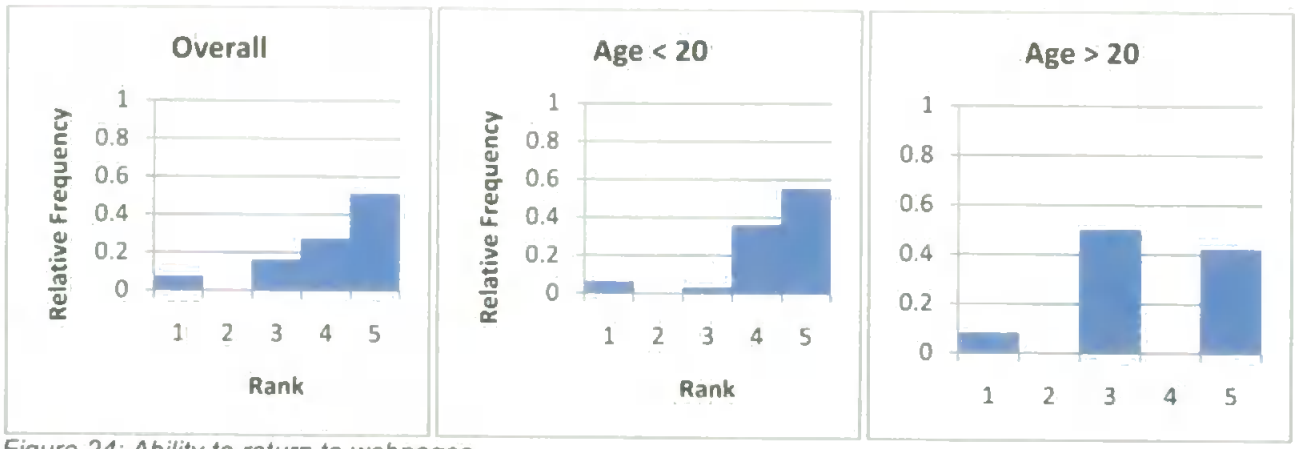


Figure 24: Ability to return to webpages

Figure 24 illustrates the overall scores achieved by this element and demonstrates that it is considered a useful approach. The interesting point to be made here is that most of those respondents in the adult category opted for the middle option, ranking of three, with others reporting their attitude at the extremes. In comparison, most of the teenagers reported themselves to be more enthusiastic about the option, giving it a ranking of five.

The discussions concerning this element illustrated some different approaches. For one teenage respondent, the facility was considered a useful tool – albeit one for deception:

> *"Useful like, when you need to go back, and like, remember what you've said where...helps keep the lies the same"*

Other teenagers considered that the usefulness lay not in being able to quantify the amount of personal information divulged, but the links whereby further validation as to the suitability of the websites could be performed. Those respondents in responsible positions, or who had close experience of abusive environments, felt that illustrating the number of websites would act as a form of deterrent. However it was suggested that the young people themselves were not likely to see a need for the list.

Display public information about self

	Overall	*Age < 20*	*Age => 20*
Min	1	1	2
Max	5	5	5
Median	4	4	3
Skew	-1.2	-1.89	0.39

Table 15: Breakdown of figures for display public information

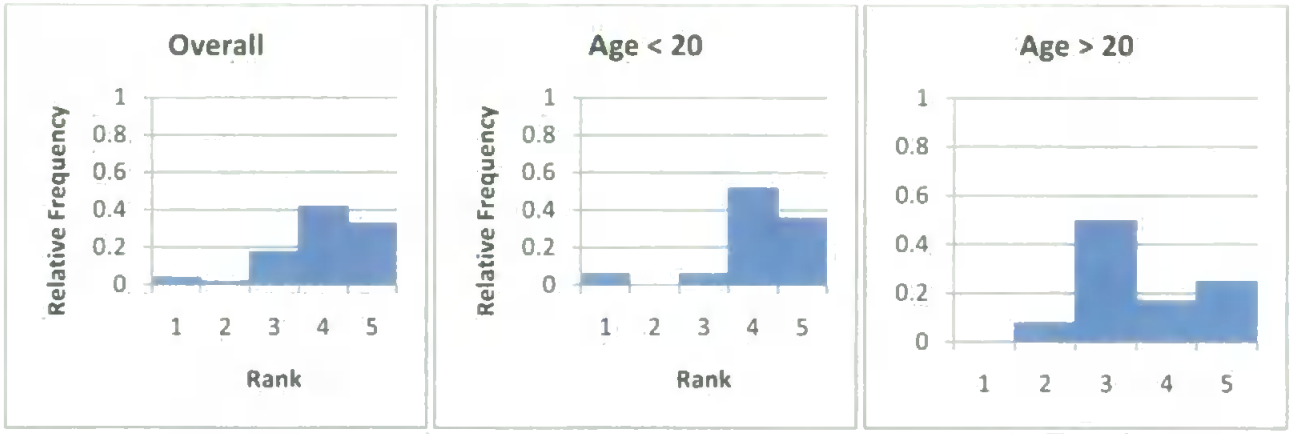


Figure 25: Display Public Information

Here the overall values illustrated in Figure 25 show that this element was considered in reasonably positive terms. However many respondents felt it merited a value of four rather than five. Within the breakdown of age groups, the adults again opted for the middle value compared to the teenage respondents predominantly valuing the element at four.

There were many positive comments, describing the feature as "cool" or "neat". Primarily respondents felt this would be a useful feature, it would serve a useful purpose for understanding what had been posted. One respondent felt it was particularly useful if frequent use was made of the Internet, suggesting that more of a mental picture could be

created.

Monitor where organisation's address divulged

	Overall	*Age < 20*	*Age => 20*
Min	2	2	3
Max	5	5	5
Median	3	3	4
Skew	0.38	0.48	0.18

Table 16: Breakdown of figures for monitoring where address divulged

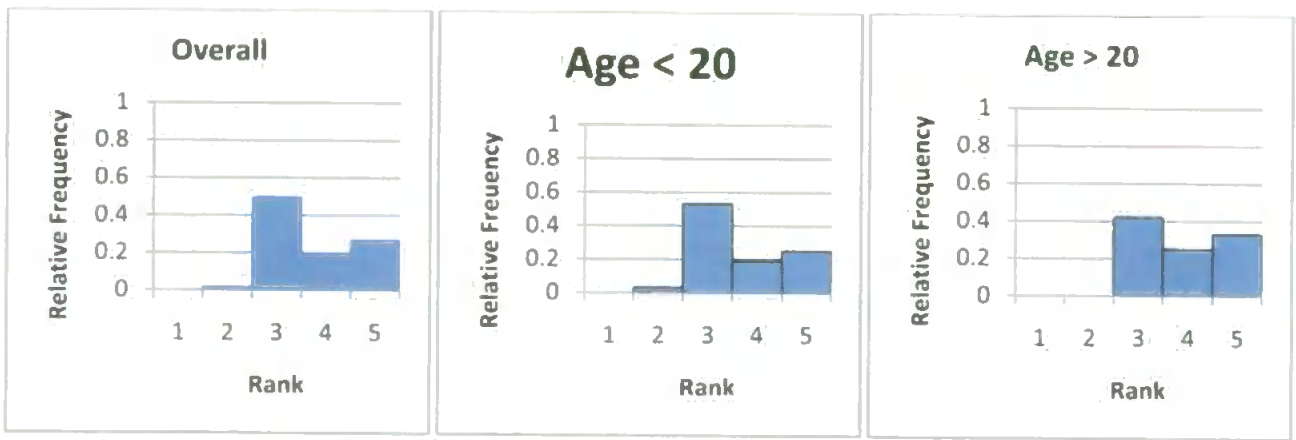


Figure 26: Monitoring Address

For this element, both the age categories follow the similar trend to the overall as can be seen in Figure 26. There is one slight exception, the oldest age category did not select any value below the mid number of three. Within the teenagers responses, values of two were the minimum reported, perhaps illustrating that some respondents felt a slightly less favourable mindset towards this particular element. It is worth remembering that the respondents in the older age category have responsibility for individuals, both teenagers and survivors, therefore they are more likely to be considering how helpful the software

would be in terms of protecting the organisation as a whole. Teenagers however, are less likely to be thinking in terms of protecting groups of them, considering themselves, rather than their school. This therefore could be seen as an indicator that they could not see the value in it rather than deeming it not to be very helpful.

The descriptive statistics were able to confirm the approaches taken within the discussions. Those respondents with a duty of care for other individuals felt that protecting the location of the organisation was an important element, whereas other respondents did not see the necessity for it. The context of the respondents emerged as an important identifier here. Respondents from refuges, essentially organisations which require a level of secrecy about their location, felt that this feature was an important layer to the complex security arrangements already in place. Respondents with responsibilities in schools felt that in their situation schools were easily found through other means, and therefore monitoring where the school address had been given out would not necessarily add to their understanding of any risks. The school address was pinpointed as an important element that deserved protection when considering the risk from paedophile activity. One respondent observed that young people were generally targeted by age and school, thus these pieces of information were important elements to monitor.

Summary of where important information divulged

	Overall	*Age < 20*	*Age => 20*
Min	1	1	2
Max	5	5	5
Median	4	4	3.5
Skew	-0.59	-0.83	-0.06

Table 17: : Breakdown of figures for Summarising

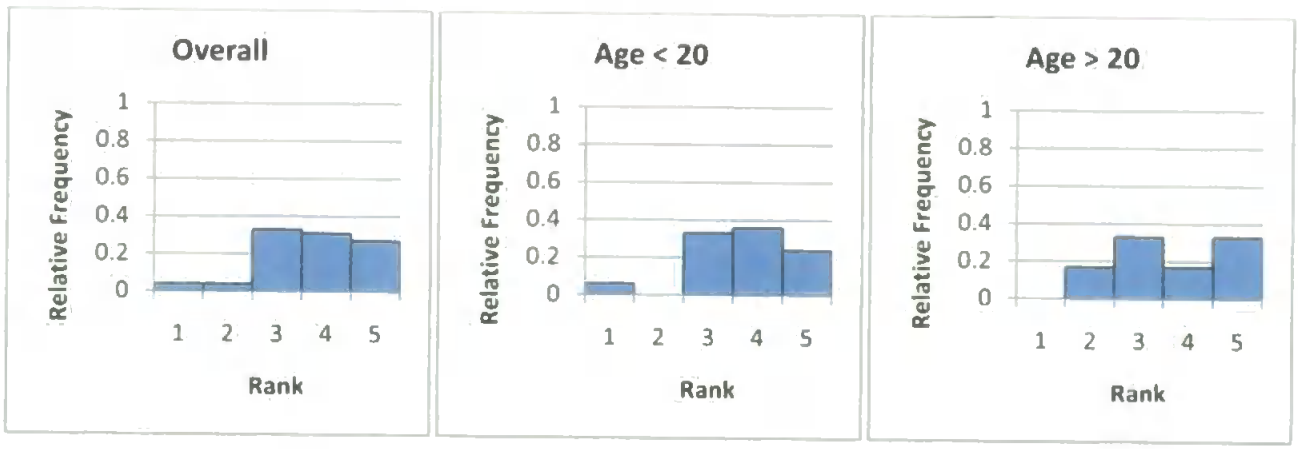


Figure 27: Summarising

The figures collected here in Figure 27 relate to the way that the amount of personal information divulged is displayed to the user of the software. A summarising bar chart illustrates for the user the relative amount of information given out in categories relating to the pieces of personal information being protected. Whilst overall the median reflects a positive attitude towards this approach, some teenage respondents awarded this a value of one suggesting that it was not very helpful at all. Other adult respondents awarded this a value of two, again suggesting it was not as helpful as it might be. The adult responses are seen to be more evenly spread, as can be seen through the low skew value. Whilst the median values have been utilised for the majority of the data reported already, a quick check for the mean and standard deviation values for these responses did support the

median value. In this category the mean value was 3.67 with a standard deviation value of 1.15.

The mixed responses discovered through the values were also reflected during the discussions and generated the most comments. Teenagers were concerned at how the software might be used as a tool of control by their parents and guardians and they voiced concern about about who would see the information gathered. One teenager considered the effect it would have on their parent:

"If it stops mum freaking out about what I put on My Space, then it's cool.. yeah... I'd use it"

Following further discussion which outlined the intention for the software to be for their use, controlled by them, one teenage respondent felt that the summary would make her think a bit more about what she was saying and where. For another teenage respondent, the concept itself was good, but they did not like the delivery, stating that they hated bar charts.

The adult respondents, however, considered a different approach. One commented that the different coloured bars allowed a clear, visual indicator of the different elements being divulged, the colours providing the emphasis required to make the elements stand out. Another comment was made about how the information was to be used, stating that:

"Schools would probably find this a very useful facility to quantify the extent of published information"

Comments were made concerning the types of information being monitored. Photographs and images were considered important elements to monitor. The point was made for some, uploading a photograph for their profile did not cause too much concern when the

pose in the photograph was quite innocent, yet for some others there were problems surrounding the more provocative poses they chose to display. Other elements suggested for monitoring were: attachments; date of birth; marital status; mobile number; email address; passwords; mother's maiden name; and the profile settings when signing up for websites to ensure that the appropriate private versus public settings were selected. One respondent was concerned about how the information was set up, suggesting that if the fields to be filled out were not mandatory, young people would not use them as they should, filling in false information, using different ways of hiding the text – for example placing spaces or asterisks within the string. Certainly the approach whereby teenagers use false information was highlighted by one of the teenage focus groups, their suggestion was that monitoring the information was not that important as most of the time they would be filling in false information on the websites.

Monitor where others names divulged

	Overall	***Age < 20***	***Age => 20***
Min	2	2	2
Max	5	5	5
Median	3	3	3.5
Skew	0.3	0.54	-0.06

Table 18: Breakdown of figures for monitoring other names

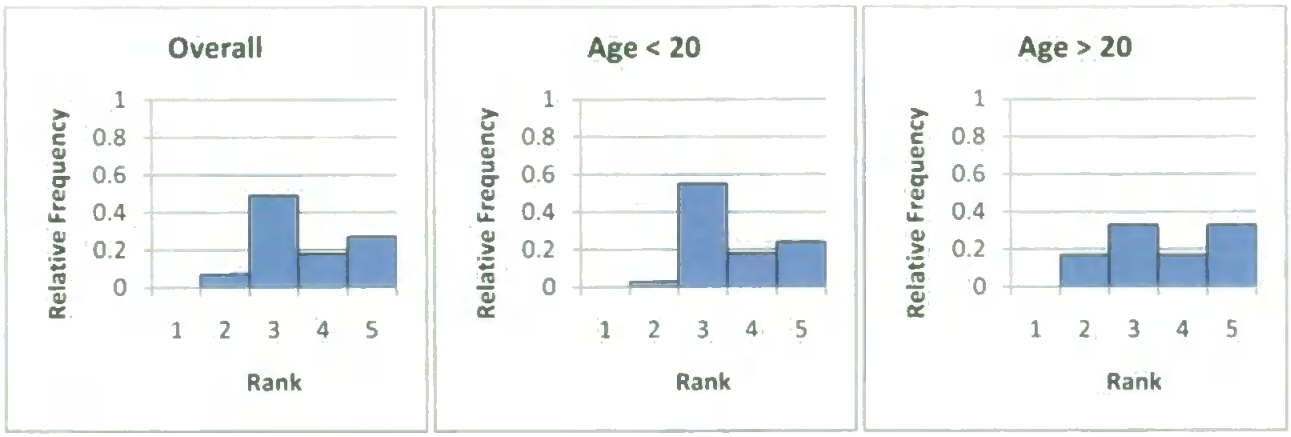


Figure 28: Monitoring Others Names

Of interest here in Figure 28, is that no minimum value of one was given by any of the respondents, all considering that this option was of some value. The teenagers tended to select the middle value, with only a few considering that the facility was very helpful. The values for the adults however, illustrated that this facility was valued more. The explanation for this may be as in the element reported above, that the adults were more aware of the requirements to protect a group of individuals, rather than for protecting just themselves.

Monitoring where work colleagues' information had been given out was considered most important within the refuge context. Concern had already been voiced about residents discussing other residents within the refuge and so this facility was considered to be a very useful protection. Whilst the prototype did not stop other peoples' names being divulged, the very fact that this was being recorded was felt to be a useful deterrent.

Traffic light indicator

	Overall	*Age < 20*	*Age => 20*
Min	1	1	2
Max	5	5	5
Median	4	4	5
Skew	-0.65	-0.54	-0.11

Table 19: Breakdown of figures for traffic light indicators

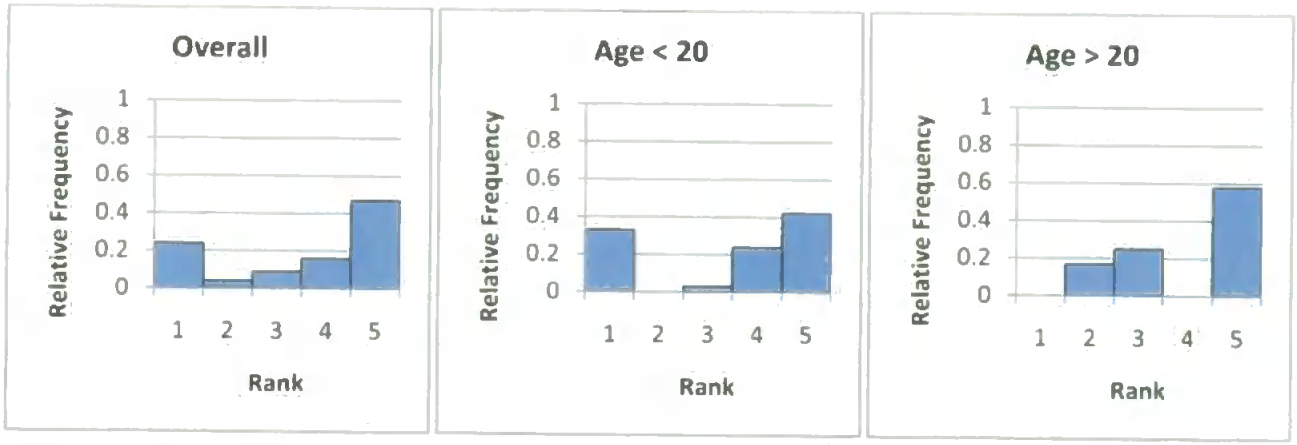


Figure 29: Traffic light indicators

Whilst the median value of four for the overall values shown in Figure 29illustrates that there is a generally favourable approach to the traffic light indicators, there are still a significant number that chose to describe this function as not being very helpful. Within the teen category it can be seen that many chose the minimum value of one, whereas no adult gave this such a low value.

The discussions surrounding the traffic light indicators were very much bound together with the evaluation of the final element, that of the highlighting of the web field. Therefore, the discussion is reported in the following paragraph concerning the web fields.

Highlighting web fields

	Overall	*Age < 20*	*Age => 20*
Min	1	1	2
Max	5	5	5
Median	3	3	4
Skew	-0.13	0.11	-0.56

Table 20: Breakdown of figures for highlighting web fields

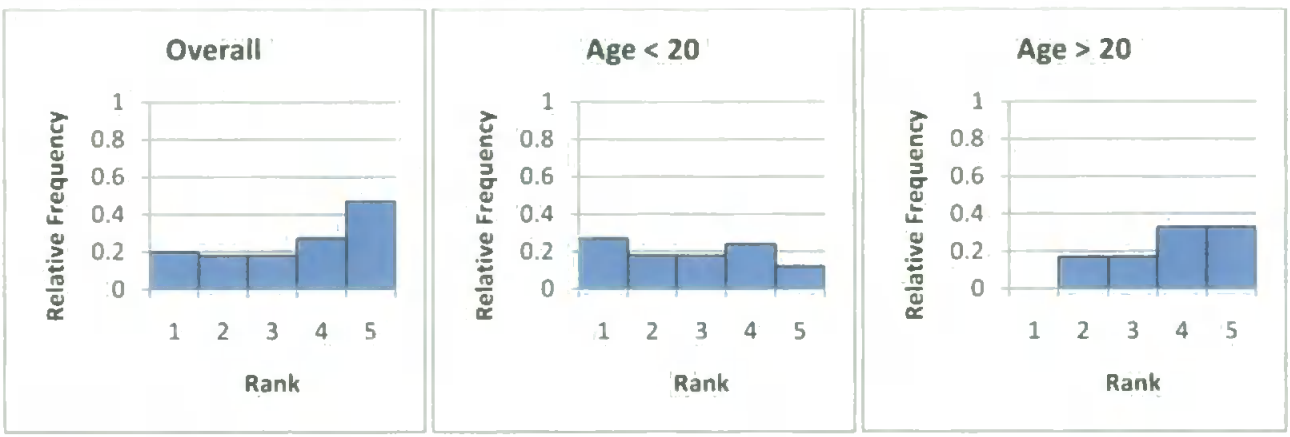


Figure 30: Highlighting webfields

The histograms for the relative frequencies here in Figure 30 illustrate a widespread opinion. Overall more people chose the value of four, whereas the median was the mid-point of three. Looking at the values between the two age groups shows that most of the teenagers did not consider this to be very helpful, whereas the adults did. There were no adults who chose the minimum value, here the minimum was given as two.

Whilst overall, the traffic light alert showing the analysis of the web page and the highlighting of any web form fields, were both ranked as the least helpful, the variety illustrated by the descriptive statistics were also reflected in the discussions and comments. The teenage respondents were quite scathing of this approach, suggesting

that both the traffic light and the highlight were irrelevant. One suggested they might consider something had gone wrong with the computer, another stated they wouldn't bother to look at it, another was a little more forceful:

"it's.... obvious from the web page, [that it is collecting information] it's ..... useless."

The adult respondents had a more mixed response, one comment suggested that the visual indicators would be a very useful indicator of potential risks. Another respondent felt that the visual indicators were more useful for those with little experience of either computers or the Internet. However, another comment considered the alerts could serve a detrimental purpose, with the wrong impression being given about sites that were essentially quite safe for young people to interact with. The suggestion was that the alert facility could create a situation whereby a young person became very anxious about what they were seeing as a privacy risk, becoming very concerned about what they should divulge, especially on a secure site, and so receiving mixed messages about what was safe and what was not. Those respondents working primarily with teenagers suggested that the alerts were likely to become easily overlooked or ignored by the young people themselves. To overcome this, popups and more expressive alerts were suggested, however, the irritation factor that these were likely to cause was acknowledged. Another suggestion made was that the alerts be based around profiling the behaviour of the person using the system. The alert would be triggered after assessing a pattern of risk taking behaviour that would be communicated to the parent or carer, with the understanding that the parent or carer would be able to discuss the issues with the young person concerned. It was questioned whether young people would engage with this approach, some

respondents felt the young people would feel they did not need to engage with this type of prototype, not believing that their divulgence of information would put them at risk.

> *"Whilst it's good, I don't think that young people would believe they needed this. They wouldn't want to be questioned about their lifestyle. People always look positively on their own experiences"*

9.5 Test Scenarios

In order to conduct further evaluation of how the prototype can assist in reducing risk, a set of two scenarios are presented below. These scenarios consider in more explicit terms exactly how the prototype tool would assist the individual to control their personal information in these given contexts. Whilst it can be argued that the incorporation of the VAF and the design of the prototype are based on the understanding of risks faced, it has to be remembed that risk is very subjective and context dependent. Therefore, these scenarios serve as further validation of the effectiveness of the approach under certain circumstances. The scenarios consider situations that the original respondent populations would face, that being of a Survivor in a refuge or a teenager in a school environment.

9.5.1 Scenario One – The Refuge

The first of these scenarios considers a Survivor in a refuge environment. It has already been established that an individual in this situation would suffer a serious risk of harm if their personal information were to be divulged (see sections 3.3 , Mental or physical harm and 4.3.1 , Selection of population). Within the VAF rating framework as illustrated in Table 11, they would be expected to score two for a high severity of consequence and a high likelihood of the event occurring. Within a refuge situation, the Survivor may be using the Internet for any form of interaction, either with existing and known websites or browsing new websites, and will be aware that the tool is monitoring the webpages and

storing where they divulge personal information.

The expected results would demonstrate a high risk alert when the Survivor navigates to a web page that is collecting personal information, especially a postcode for example. This high risk alert manifests itself as a red circle in the toolbar and the field on the web form collecting the postcode highlighted red. In addition, the details of where the Survivor has posted information about their refuge address should also be collected and displayed when required.

The actual results of the prototype matched the expected results: a red circle was displayed, the postcode field was highlighted in red and the information about where the information was divulged recorded for evaluation. Based on the user-group evaluations it can be demonstrated that the effect of the tool would be to get people thinking. As discussed earlier in this section, respondents found utility in the mental picture created by the tool; the monitoring of the address, of other individuals, and the traffic light indicator all achieved a high rating by the adults. Specifically, one respondent reported that aggregating the data in this fashion would be a useful deterrent to Survivors giving out not just their own personal information, but also the information of others within the refuge.

9.5.2 Scenario Two – The School

In this scenario, a teenager who is prone to being bullied makes use of the tool when browsing the Internet. It is set up as an established tool for use within the school environment and all computers within that environment have this monitoring tool incorporated into the browser. The established risk of harm to the teenager is that from

bullying, stalking or predatory sexual attack (see sections Mental or Physical Harm 3.3 , Mental or physical harm and 4.6.1, Selection of respondents). For this scenario, the teenager is allocated a score of one from the VAF Assessment Matrix shown in Table 11, being created from a risk assessment of having a high likelihood of happening and a low severity of consequence.

The expected results would be that as the teenager navigates to a website collecting personal information, the toolbar shows a yellow circle and the web fields collecting names shows a yellow background. In addition, the details of where other teenagers within the school have posted information about their classmates should also be collected and displayed when required.

The actual results were not exactly as expected. The yellow circle is shown, but the postcode field shown on the test page is still shown with a red highlight background. The reasoning behind this is because the postcode is still considered to require a high level of protection irrespective of the rating of the individual. Taking the user group evaluation however, this might not be a suitable approach. The teenagers did not rate either the traffic light indicator or the highlight for the web field background as very useful. It was also suggested that these alerts could serve a detrimental purpose for young people, generating more concern than was necessary. This should be taken in balance with the other comments that demonstrated that the monitoring of where personal information was being divulged along with the ability to return to those websites would assist the users in their understanding of potential risks. The display of where names were divulged would

highlight where other members of the class had divulged the teenagers' name, assisting in pinpointing where bullying behaviour was occurring.

9.6 Conclusion

The evaluation conducted took two separate approaches. The first sought to ground the evaluation in the real world by taking specific user opinion, the second took a more theoretical approach with the application of specific scenarios. The user opinions served a useful purpose to gain an overview of the acceptability of the prototype. By considering in theory how the prototype would behave in each scenario, then setting out to replicate that scenario, allowed an evaluation of a more fine-grained and specific nature to be conducted.

The findings from the discussions and the questionnaire illustrate quite clearly the tension that lies between the individual users of the software and those who have a duty of care for them. Teenagers were concerned where the control actually lay, did it lay with them or externally with parents. Despite this concern, the difference between their rating of the software and the adults rating did not illustrate a marked difference, with both age groups being positive overall.

Whilst the Likert scales utilised here were useful to provide pointers, more in depth analysis could be provided by adopting a different approach. Further work is discussed later in more detail in chapter 10 when consideration would be given to longitudinal experiments with user groups measuring the prototype effects on the amount of personal information divulged. It is entirely likely that the adults with a duty of care for individuals

have reported in a risk averse fashion and therefore have a tendency to select the middle value.

The analysis of the elements of the prototype in more depth allowed a view to be taken on the differences between the adults and the teenagers. This can allow consideration as to how control of personal information might be utilised in a fashion that is more acceptable to teenagers.

The findings of the evaluation data, that of the overall positive response, confirm the original hypothesis:

> *The more favourable the attitude, the more likely it is that the software will be used. Individuals are therefore more likely to exert control over their own personal information which will in turn reduce their vulnerability.*

This would suggest that individuals would be happy to have their personal data monitored during their interactions with the Internet, provided they had control over the monitoring.

The test scenarios demonstrated how the findings, combined with the evaluations from the user-groups, could act upon the behaviour of the individual to restrict the amount of information being divulged. The Survivor would be deterred from giving out information because of the alerts, and the tool can assist with addressing bullying behaviour within the school environment by monitoring where information about other individuals is divulged. Based on the opinions of the users consulted, this approach would appear to provide a deterrent and therefore reduce the risk. This is a tentative conclusion, because further

research would be required to discover if this is indeed a fact, however it does take the protection for harm a step closer.

This combined approach of both social interaction and theoretical considerations illustrates quite clearly how the balance between socio and technical elements can be achieved through a careful combination of relevant theoretical approaches. Despite the paucity of relevant literature describing the inter-disciplinary approach, as illustrated in Figure 3, the prototype is a tangible demonstration that the research methods were able to address the three objectives originally described in section 4.2 of:

- adapting to offline and online context;
- exploring the complexity of the context; and
- demonstrating an understanding of the risks in a format useful for software design.

The theoretical approaches selected provided an equal contribution to the overall research design which contributed to a rich understanding of the context. Each had an important and highly relevant bearing on the area of research, that of mitigating the risk posed to individuals from the release of personal information. The whole ethos of the research and prototype designs illustrated clearly that ethical considerations and an understanding of the experiences of the marginalised could be used alongside the design and action theories for information systems. From this combination of theoretical approaches, a suitable and acceptable prototype was created. The evaluation data demonstrated the

acceptability and the scenario theorising demonstrated the suitability given specific circumstances. Therefore a key learning point is that the domain under scrutiny should be carefully assessed to determine what relevant theoretical considerations have an influence, prior to considering how to combine them.

Considering the prototype in a more specific fashion however, the limitations of the VAF demonstrated clearly the difficulty in adapting a piece of software to suit the context of different individuals. As it stands now, the VAF is not fine grained enough to serve the purpose, as can be seen in the applied scenario with the teenager and the postcode field still being highlighted in red. Currently the VAF allocates a rating to each element of personal information, scaling this up to an overall rating adds a complexity that requires further consideration. Incorporating a more robust and fine-tuned reasoning approach is discussed in the further work section in chapter 10 , which should address this lack of adaptability to context. However, this relies upon further reasoning tools being developed that are easy to incorporate into software design and implementation. This is an area that the ontological reasoning element of the Semantic Web hopes to address.

As has been demonstrated throughout this research, complex social constructs such as privacy require fairly complex theoretical frameworks within which to examine them. Complexity however need not be a barrier, but serves to assist in gaining an understanding. The results from the evaluation presented here demonstrate this is achievable. The achievements of the research are further articulated in chapter 10

10 Conclusion

This chapter concludes this thesis by considering the achievements of this research and follows with consideration of the limitations. The chapter proceeds with a discussion on future work prior to concluding with a personal review of privacy.

This research set out to explore how technology could address the issues arising from the potential for harm emerging from the effects of Internet technologies on personal data. To effectively create a technological support tool, an understanding of the privacy situation as a whole was required. This meant an effective strategy needed to be put into place, created from three separate strands of knowledge.

1. The first was to conduct an effective review of the field of personal privacy, exploring the issues and the problems as currently known.
2. The second was to understand how to conduct effective research in a fashion that accounted for the viewpoint of individuals, and so a review was carried out of qualitative methods and an appropriate epistemological framework.
3. From here, the application of findings evolved into a holistic, human-centred approach to software design, first providing assessment tools to address risks.

As is common with qualitative techniques, it was difficult to generalise the findings. Therefore a conceptual framework emerged from the analysis that served as a useful tool for risk assessment, and was further validated by its application in two separate areas.

The development of the results into a software prototype involved addressing complexity issues surrounding the adoption of the Semantic Web, an approach in its early stages. The prototype demonstrated however that a supportive, acceptable tool for use by the end user, that did not require explicit choices surrounding levels of privacy protection, could indeed be created and accepted.

10.1 Achievements of Research

In an earlier chapter of this thesis, chapter 3, the issues surrounding the divulging of personal information were discussed, with a special emphasis on the issues of vulnerability and the inequitable distribution of privacy risks. The findings from this research programme have challenged current technological approaches to privacy protection and posited the approach that the individual should be empowered and supported to assist themselves in controlling their own personal information. Therefore the achievements of the programme can be viewed in terms of progressing understanding related to the design of technologies for the individual.

Additionally, the achievement of the objectives outlined in the introductory chapter of this thesis can be seen to have contributed effectively to the field of risk reduction. These objectives are discussed in turn:

1. To gain a clear understanding of risks and the distribution of risks.

By gaining a clear understanding of the risks with a specific focus on the distribution of

risks posed to vulnerable individuals, this research has been able to contribute effectively to relevant safety planning for the groups concerned. Two publications in the Women's Aid journal brought to the fore issues surrounding technologically-mediated stalking. In addition, four separate workshops run at the Women's Aid conferences of 2006 and 2007 assisted attendees in effective safety planning, accounting for the influences that Internet technologies were having on the users of their services.

2. To develop a taxonomy framework to assist in the identification of risks;

Developing the taxonomy framework provided a novel, and relevant, tool for use in risk assessment, bringing a supportive framework for individual risk assessors requiring direction when considering risks. The taxonomy provides a common conceptual model by which practitioners can discuss more effectively dangers faced in their fields. It also provides a loose enough framework so that their risk assessment approaches are not restricted.

3. To develop a design for software that allows for technological control of personal information, adaptable to the context of the individual;
4. To implement a prototype of the design;
5. For user-groups to evaluate the prototype in order to gain an understanding of the acceptability of such a software solution.

The prototype design, implementation and evaluation provided evidence that a novel combination of theoretical approaches could contribute effectively to the body of

knowledge. This cross-disciplinary approach, allowing elements from the four theoretical domains of software engineering, information systems, social science, and criminal behaviour to contribute equally, has led to an effective research design. Social factors were able to influence technological design in such a way that resulted in a piece of software acceptable to the individual: an approach often dismissed by the technological community, yet fully advocated by the sociotechnical community. Whilst the combination of theoretical approaches would at first appear quite complex, privacy is in itself a complex issue influenced by many and varied factors, as discussed in chapter 2. Therefore, the adoption of any one theory that has a fairly narrow focus does not do the research any justice. The novel contribution that this research provides is that the complexity should not be a barrier to research, nor should it be avoided, but should be reflected in the selection and combination of theoretical underpinning.

The resultant evaluation of the prototype led to a positive outcome whereby teenagers, despite the tension demonstrated between them and the adults, deemed a monitoring approach adopted by the prototype to be acceptable – provided the control lay with the individual. Combining the user evaluations with the test scenarios demonstrated the strength of the prototype for raising awareness of the potential risk for people posting information online. The test scenarios outlined how the prototype would affect an individuals' behaviour in certain circumstances and the respondents' opinions confirmed that the software would act upon the behaviour of the users, thus reducing the risk of harm from divulging personal information.

Each of the steps within the research programme provided an incremental approach to

understanding and addressing the risks that Internet technologies bring to the individual. The understanding gained from using qualitative techniques in the exploration of the social context of privacy, provided the social context with an equal stake in the research design. This in turn provided a firm basis from which to create assessment frameworks and these frameworks formed part of the prototype development and implementation. This illustrated clearly that a combination of approaches was necessary to provide the protection for the individual with the prototype as an end product. The prototype demonstrated that technology could be acceptable as a tool for protection, but only when social context is given enough credence and room, an approach advocated by the socio-technical community and discussed in section 4.2 . This research design therefore demonstrates how effective an equal balance of social context and technological design can be at creating an acceptable and suitable prototype.

10.2 Limitations

Despite all the objectives of this research programme having been met, there are a number of limitations to the research. The key limitations are summarised below:

- Insufficient time for further assessment. Time and financial constraints meant that young people were only accessible during term time, and not at times when heavy examination workloads were prevalent. Once the summer terms had ended in the schools, the young people had left for their holidays and were not contactable. The prototype evaluations were not able to be carried out in great depth, there were no opportunities to observe the use of the prototype in a real life situation or over a period of time.

- Software constraints. The prototype was developed only for the Internet Explorer browser which, as was discussed in the earlier chapters, is not the only means of interaction with the Internet. Other methods of divulging personal information were not able to be included within this prototype software. Utilising elements of the Semantic Web posed limitations in that these techniques are not yet mainstream and ontological development in the field of personal privacy is not a mature enough field to be incorporated into the prototype. In addition, the approach of describing the purpose of a webpage is not in use, therefore the querying mechanism to evaluate the web pages is not entirely suitable. The processing of the RDF files was also restricted by the choice of RDF parser, as these become more commonplace and established it is anticipated that more could be achieved with the reasoning elements of the prototype.
- VAF not fine-grained enough to adapt to context. Whilst the taxonomy of threat devised from the concepts of risks was a useful tool for risk assessors, incorporating the taxonomy fully into the VAF was not as effective as it should have been. The effect of this was shown when exploring the applied scenarios in the evaluation section 9.5.2, and alluded to in one of the respondents' discussions surrounding the potential for the alert mechanism to create more anxiety. In this particular instance, it can be seen that the technological approach is weaker than the sociological approach, and therefore needs further work.

Despite the limitations, the research programme has been able to demonstrate a valid contribution to knowledge and provided sufficient proof-of-concept for the ideas posited in

the earlier sections of this thesis, thus proving that social and ethical considerations can be effectively incorporated into a holistic software assisted approach.

10.3 Future work

Building upon this research programme the following is proposed as further work.

- Conduct a longitudinal study into the effectiveness of the prototype. Whilst initial feedback for the prototype has been very positive, it has not been tested by users engaging with the software directly or for any period of time. The evaluation carried out only measured perceptions of safety, rather than actual safety. Further work is required to measure the effectiveness of the prototype as a protective mechanism. The feedback gained here could be utilised to further strengthen the prototype to make it more robust. Respondents could then be invited to a controlled experiment which took measures of personal information being divulged prior to engaging with the software. The next step could be to conduct a longitudinal study where the respondents utilised the software during their everyday interactions, recording the limitations surrounding their usage. A measure taken at the end of the study would determine the effect of the prototype, it's success being measured in a decrease in the amount of information being divulged. Another measure of success would be to record situations where privacy issues needed to be addressed and to assess whether the information provided by the prototype had been beneficial to the individual.
- Further develop the Semantic Web component. The prototype could be further developed to embrace more of the Semantic Web techniques, putting more

reasoning into the computation. For example, the VAF framework could be extended with further triples to describe more data than is currently used and to provide for more robust reasoning. This could include the establishment of acceptable privacy approaches, for example tools enabling web developers to describe the types and elements of personal information that their web pages are collecting.

- Incorporate into existing research approaches. Existing P3P privacy research along with Semantic Web agent research could be adopted into this prototype. This could provide for the development of acceptable industry wide ontologies along with industry based software that incorporates Semantic Web agents. These software agents could perform negotiations with a Semantic Web agent incorporated into the prototype to act as negotiators for an agreed approach to privacy.
- Develop the prototype for alternative methods of interaction. The prototype is currently limited to use in the Internet Explorer 7 browser. Not only could this be developed for alternative browsers, but could also be developed for separate devices and interactions with the Internet. As discussed in chapter 2, there are many ways of interaction with the Internet and there may be further utility in adapting the prototype for use on mobile phones, virtual worlds, instant messaging and email.
- Develop taxonomy for privacy impact assessment. The taxonomy could be developed further to be used in alternative privacy assessments. Research could be conducted to tailor the taxonomy to separate domains prior to testing for suitability. Feedback could be utilised to further develop and improve the

taxonomy.

- Detection of abusive behaviours. Cross-disciplinary research including the criminal justice field and the psychology fields, could be conducted to determine if the prototype could be utilised to ascertain patterns of behaviour where bullying or abusive behaviours were occurring Further work could also include incorporating visual or audio support for protecting vulnerable individuals.

10.4 Privacy Review

Privacy for the individual has changed dramatically during the three years of conducting this research programme. At the beginning there was little evidence of concern about the way personal information could be easily shared and divulged, and the methods by which young people interact with the Internet had not become so prominent. Privacy of information was not then high on the media agenda.

Since the beginning of this research programme the field has changed and this has proven to be a fast moving domain. The incorporation of child protection into the Internet has become prominent, through both media stories and government activity. The more established social networking applications along with established methods for communication have altered their safety messages to incorporate prominent child protection measures.

Increasingly the developers of technology are becoming aware of the need to protect personal information, although it yet remains to be seen how that awareness is being

translated into action. Indeed at a recent conference on Internet Technologies, the keynote addresses were focused on social factors.

However, there is still a perceptible divide; a gap. There is a gulf between those who traditionally concentrate on sociological approaches and those who concentrate on technological approaches. Each are correct in their own field, but something, somebody needs to fill the gap and build the bridge between them. People who understand both sides, both approaches, and can communicate and understand effectively in both those fields are needed. Between these two domains there is the need to accept and support each other, for each has their place. This inter-disciplinary field provides for an important element in protecting privacy for the individual. By bridging the gap and providing the link, privacy can be seen to be improved, and thus reducing the harm to individuals.

Privacy for the individual is likely to grow as a field of concern. Whilst there are approaches whereby business concerns are looking to gain consumer trust by their practices, there is still a need to focus on how the individual can be assisted to help themselves. This research provides one viewpoint on how this could be addressed. The prototype is a tool for use by the individual and represents the final manifestation of a series of stages. The first stage began with the ethical consideration of the experiences of those often marginalised (Survivors and teenagers), with the understanding gleaned through sympathetic data collection. During the next stage, the tool built upon a risk management paradigm which was oriented towards a change in approach, that of influencing the cognitive behaviour of the individual. The final stage saw the

implementation of the tool, resulting in a balance between the social context of privacy and the harnessing of the new technological approach of the Semantic Web to provide an acceptable and suitable tool for the individual. Therefore, this research has demonstrated that technology can be used to assist privacy concerns for the individual, rather than exacerbate their problems.

11 References

AIFB, (2006), Research Group Knowledge Management, http://www.aifb.uni-karlsruhe.de/Forschungsgruppen/WBS/english

Altova, (2006), Altova Semantic Web Tools, http://www.altova.com/dev_portal_semanticweb.html

Alwang, J., Siegel, P.B., Jorgensen, S.L., (2002) Vulnerability as viewed from different disciplines. In proceedings of International Symposium Sustaining Food Security and Managing Natural Resources in Southeast Asia.

Anderson, K.B., (2006) Who are the victims of identity theft? The effect of demographics, JOURNAL OF PUBLIC POLICY & MARKETING 25 (2): 160-171 FAL 2006

Anderson, R., (2006), Under threat: patient confidentiality and NHS Computing, In Drugs and Alcohol Today, v6, No 4, (Dec 2006), pp 13 – 17, http://www.cl.cam.ac.uk/~rja14/Papers/drugsandalcohol.pdf

Anton, A.I., Earp, J.B., Reese, A., (2002), Analysing Web Site Privacy Requirements Using a Privacy Goal Taxonomy, In Proceedings of 10th Anniversary IEEE Joint Requirements Engineering Conference (RE'02), February 2, 2002,

APACS, (2007) Card Fraud Facts and Figures, http://www.apacs.org.uk/resources_publications/card_fraud_facts_and_figures.html

ARCH, (2007),The Children's Information Sharing (IS) Index, http://www.arch-ed.org/issues/databases/IS%20Index.htm

Arnold et al, (1995), Ethical Issues in Biological Psychiatric Research with Children and Adolescents, Journal of the American Academy of Child and Adolescent Psychiatry, Volume 34, Issue 7, 1995, pages 929-939

Ashby, W.R., (1958), Requisite Variety and its implications for the control of complex systems. Cybernetica (Namur) Vol1, No 2, quoted in Heylighen, F., (1992) Principles of Systems and Cybernetics: an evolutionary perspective, in Cybernetics and Systems '92. R. Trapple (ed) World Science, Singapore, p3-10.

Atkinson S, Johnson C, Phippen AD, (2007), Personal Privacy Threats: A Taxonomy for Risk Assessment. In Proceedings of Second International Conference on Internet Technologies and Applications

Avison, D.E., Fitzgerald, G., (1995), Information systems Development: Methodologies, Techniques and Tools 2nd Ed., McGraw-Hill, Berkshire

Backgroundchecking, (2007), Background Checking Solutions, , http://www.backgroundchecking.com

Bachlechner, D, (2006), Research at Deri, Deri, Ireland, www.deri.ie/research/projects

Bakardjieva, M, (2005), Internet Society: The Internet in Everyday Life, Sage Publications, London,

Ball, L.J. & Ormerod, T.C. (2000). Putting ethnography to work: The case for a cognitive ethnography of design. International Journal of Human-Computer Studies, 53, 147-168.

Ballard, M, (2006), Home Office thumbs up for Yeovil pub fingerprint plan. The Register, 26 October 2006, http://www.theregister.co.uk/2006/10/26/pub_fingerprint_plan/

Bartow, A, (2000), Our Data Ourselves: Privacy, Propertization and Gender, University of San Francisco Law Review, University of San Francisco School of Law

Baruch, Y., (2005), Bullying on the net: adverse behavior on e-mail and its impact, Information and Management Volume 42, Issue 2 (January 2005) Pages: 361 - 371

Basbas, S, (2006), The Impact of e-commerce on Transport, In Proceedings of The Internet and Society II, (Eds) Morgan, K., Brebbia, C.A., and Spector, J.M, WIT Press, Southampton

Baskerville R. And Land, F.(2004), Socially self-destructive systems" in Avgerou, C., Ciborra, C., Land, F. (2004) The Social Study of Information and Communication Technology: Innovation, Actors and Contexts. OUP.

BBC, (2002), Schools ban mobile phones, Tuesday 8 January 2002, http://news.bbc.co.uk/1/hi/education/1748527.stm

BBC, (2004), Google's Gmail could be blocked, Thursday, 13 April, 2004 http://news.bbc.co.uk/1/hi/business/3621169.stm

BBC, (2006a), Giant ID computer plan scrapped. http://news.bbc.co.uk/1/hi/uk_politics/6192419.stm

BBC, (2006b), YouTube moves to the small screen, BBC, 28 November 2006http://news.bbc.co.uk/1/hi/technology/6190984.stm

BBC, (2006c), blogging set to peak next year , BBC, 14 December 2006 http://news.bbc.co.uk/1/hi/technology/6178611.stm

BBC, (2007), Taking cover from ID theft, BBC, 22 November 2007, http://news.bbc.co.uk/1/hi/magazine/7107243.stm

BBC, (2007a), NHS 'can be trusted' over records, BBC, 24 December 2007, http://news.bbc.co.uk/1/hi/uk/7158688.stm, accesed December 2007

BBC, (2007b), Discs 'worth £1.5bn' to criminals, BBC, 28 November 2007, http://news.bbc.co.uk/1/hi/uk_politics/7117291stm, accessed December 2007

Beaumont, C., (2007) Facebook bows to user pressure in privacy row. Telegraph, 30 November 2007, http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/2007/11/30/dlface30.xml
Beckett, D., (2007), Redland RDF Libraries, http://librdf.org/

BECTA (2004) Data Protection and Security, Coventry, BECTA

Beeble, M.L., Bybee, D., Sullivan, C.M., (2007) Abusive Men's Use of Children to Control Their Partners and Ex-Partners, European Psychologist, Volume 12, Issue 1, March 2007, Pages 54-61

Bennett, C.J, (1997), Convergence Revisited: Toward a Global Policy for Protection of Personal Data, In Technology and Privacy: The New Landscape, Agre, P.E., and Rotenberg, M (Eds),, MIT Press, London

Berners-Lee T, (2000), Weaving the Web, Texere, London

Bibby, A., (2007), Your identity, lying on the doorstep, The Guardian, 25 March 2007 http://money.guardian.co.uk/scamsandfraud/story/0,,2042130,00.html

Bilton et al, (1987), Introductory Sociology 2nd Ed, Macmillan Press, Basingstoke

Blodget, H., (2007) Compete CEO: ISPs sell clickstreams for $5 a month. Seeking Alpha, http://internet.seekingalpha.com/article/29449

Blunkett, D, (2004), ID card pilot scheme under way, 10 Downing Street, 26 April 2004 http://www.number-

10.gov.uk/output/page5701.asp

Bocij, P.., (2004a), Cyberstalking: Harrassment in the Internet age and how to protect your family. Praeger, Westport.

Bocij, P, (2004b), Cyberstalking, Praeger, Conneticut

Boehm, B., (2004) The role of empiricism in software engineering. http://ese.uniroma2.it/events/eseiw2003/eseiw1.htm

Boland, R., (1985) Phenomenology: A preferred approach to research on information systems, in Mumford, E., Hirschheim, R., Fitzgerald, G., and Wood-Harper, T (eds), Research Methods in Information Systems. Amsterdam, North-Holland, pp193-201

Bolman, C, (2006), Youngsters Often Victims of Cyberbullying, Open University Netherlands, InSafe, Monday, 12 Jun 2006 http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0606/oun.htm

Boulos, M.N.K., Wheeler, S, (2007), The emerging Web 2.0 social software: an enabling suite of sociable technologies in health and health care education, Health Information and Libraries Journal 24 (1), 2–23.

Brennan, M., (2006), Understanding Online Social Network Services and Risks to Youth, http://www.ceop.gov.uk/pdfs/Social%20network%20serv%20report%20221206.pdf
Briggs, D., Doyle, P., Gooche, T., Kennington, R., (1998), Assessing Men who Sexually Abuse, Jessica Kingsley, London.

Bryman, A, (2004), Social Research Methods Second Edition, Oxford University Press, Oxford

Burkett, H, (1997), Privacy-Enhancing Technologies: Typology, Critique, Vision, In Technology and Privacy: The New Landscape, Agre, P.E., and Rotenberg, M (Eds),, MIT Press, London

Byers, S., Cranor, L., Kormann D and McDaniel, P, (2004), Searching for Privacy: Design and Implementation of a P3P-Enabled Search Engine, In Proceedings of the 2004 Workshop on Privacy Enhancing Technologies (PET 2004), Toronto, Canada, http://lorrie.cranor.org/pubs/pets04.html

Cabinet Office, (2000), UK Online Annual Report, 2000, http://archive.cabinetoffice.gov.uk/e-government/docs/annualreports/2000/AnnualReport2000.pdf

Cabral, L,.., Domingue, J., Motta, E., Payne, T., Hakimpour, F, (2004), Approaches to Semantic Web Services: an overview and comparisons, In LNCS 3053 pp225-239, Vol 3053, pp225-239, Springer-Verlag, Germany,

Cannon, J.C., (2004), Privacy What Developers and IT Professionals Should Know, Addison Wesley Professional, Harlow

Carins, R, (2005), Credit Checks and Your Job, Fresh Finance, http://www.freshfinance.net/articles-creditchecksjob.htm

Carr, M.J., Konda, S.L., Monarch, I., Ulrich, F.C., Walker, C.F., (1993), Taxonomy-based Risk Identification, sei.cmu.edu, http://www2.cs.uh.edu/~zhibinma/tx.pdf

Catan, T, (2006), Bullies move into cyberspace, The Times Online, retrieved November 2006 http://www.timesonline.co.uk/article/0,,13509-2457146,00.html

Cavoukian, A., Tapscott, D, (1997), Who Knows, McGraw-Hill, USA

CEOP, (2007), Child Exploitation and Online Protection Centre, http://www.ceop.gov.uk/

CFH, (2007), Connecting for Health, http://www.connectingforhealth.nhs.uk/systemsandservices/nhsnumber/

Charlton, T., C. Panting and A. Hannan (2002) Mobile telephone ownership and useage amongst 10- and 11-year-olds: participation and exclusion. Emotional and Behavioural Difficulties 7.3, 152–63.

Checkland, P., Scholes, J., (1999), Soft Systems Methodology in Action, John Wiley and Sons Ltd, Chichester

Chellappa, R.K., Gin, R.G, (2005), Personalization versus Privacy: An Empirical Examination of the Online Consumers Dilemma, Information Technology and Management , Volume 6, Numbers 2-3

Chen, H., Wu, Z., (2003), OKSA: An open knowledge service architecture for building large scale knowledge system in semantic web, Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, v 5, 2003, p 4858-4863,

Chen, H., Finin, T., Joshi, A., (2004), Semantic Web in the context broker architecture, In Proceedings - Second IEEE Annual Conference on Pervasive Computing and Communications, PerCom 2004,, p 277-286,

Chen, Y., Chen, P.S., Hwang, J., Korba, L., Song, R., Yee, G., (2005), An analysis of online gaming crime characteristics In Internet Research, Jul 2005 Volume: 15 Issue: 3 Page: 246 - 261, Emerald Group Publishing Limited

Chen, VHH, Duh, HBL, Phuah, PSK, Lam, DZY, (2006), Enjoyment or engagement? Role of social interaction in playing Massively Mulitplayer Online Role-playing Games (MMORPGS), ENTERTAINMENT COMPUTING - ICEC 2006 4161: 262-267, 2006

Chik, W.B., (2005) The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on the Internet. International Journal of Law and Information Technology, Oxford University Press, 2005

ChildNet, (2007), Young People, Music and the Internet, www.pro-music.org/guide

Chisholm, J.F., (2006), Cyberspace Violence against Girls and Adolescent Females, Annals of the New York Academy of Sciences 1087 (1), 74–89.

Ciborra, C., (2006), Imbrication of Representations: Risk and Digital Technologies, Journal of Management Studies 43 (6), 1339–1356.

CIFAS, 2007, 2006 – FRAUD TRENDS, http://www.cifas.org.uk/press_20070130.asp

CIFAS, (2007a), Identity Theft – Victims, http://www.cifas.org.uk/default.asp?edit_id=577-73

CIOC, 2007, Transformational Government Annual Report 2006, Chief Information Officer Council, http://www.cio.gov.uk/transformational_government/annual_report2006/index.asp

Clark, C., (2001), Why Brass Eye got it right. Times Higher Education Supplement, 3 August 2001. http://www.ncl.ac.uk/press.office/press.release/content.phtml?ref=996767710

Clarke, R, (1999), Introduction to Dataveillance and Information Privacy, and Definitions of Terms, Xmamx Consultancy Pty Ltd, http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#Intro

Clarke, R.V., (2000), Situational Prevention, Criminology and Social Values, In Hirsch, A., Garland, D., Wakefield, A., (2000) (Eds) Ethical and Social Perspectives on Situational Crime Prevention, Hart, Oxford.

Clarke, R.V., and Cornish, D.B., (2004), Opportunities, precipitators and criminal decisions: A reply to

Wortley's critique of situational crime prevention. Theory for Practice in Situational Crime Prevention, Crime Prevention Studies, Vol 16, 2004.

Clarke, R., (2007), The Feasibility of Consumer Device Security, http://www.anu.edu.au/people/Roger.Clarke/II/ConsDevSecy.html#CD

Clegg, C.W., Sociotechnical principles for system design, Applied Ergonomics, Volume 31, Issue 5. 2 October 2000, pp463-477

Coakes, E., Willis, D., Lloyd-Jones, R, (2000), The New SocioTech, Springer, London

Collins, J, (2005), Marks & Spencer to Extend Trial to 53 Stores, RFID Journal, http://www.rfidjournal.com/article/articleview/1412/1/1/

Colvin, M, (2002), Developing Key Privacy Rights, Hart Publishing, Oregon

Connor, S., (2005), Britain will be first country to monitor every car journey, The Independent, 22 December 2005, http://news.independent.co.uk/uk/transport/article334686.ece.

Cooper, A., (2004), The Inmates are running the asylum. SAMS, USA

Council of Europe, (1950) European Convention for the Protection of Human Rights and Fundamental Freedoms, Romse, 4.XI.1950, http://conventions.coe.int/treaty/en/Treaties/Html/005.htm accessed 19 May 2007

Cranor, L. F. and J. Reidenberg (2002). Can user agents accurately represent privacy notices? The 30th Research Conference on Information, Communication, and Internet Policy, Alexandria, Virginia, USA.

Cranor, L.F. and Garfinkel, S, (2005), Security and Usability, O'Reilly, USA

Cresswell, J.W., (1994), Research Design: Qualitative and Quantitative Approaches. Sage. California.

Cresswell, J.W., (1998), Qualitative Inquiry and Research Design. Sage. California.

CRU, (2007), Cyberspace Research Unit, University of Central Lancashire, http://www.uclan.ac.uk/host/cru/index.htm

Cubrilovic, N., (2007), Yahoo! Launches Pipes, TechCrunch, http://www.techcrunch.com/2007/02/07/yahoo-launches-pipes/

Culnan, M., Bies, R.J., (2003), Consumer Privacy: Balancing Economic and Justice considerations, Journal of Social Issues, Vol 59, No 2, 2003, pp323-342

Curry, A, (2005) Action Research in Action: Involving Students and Professionals. In proceedings of World Library and Information Congress, Oslo, Norway. 14 – 18 August 2005

Davies, L., Ledington, P, (1991), Information in Action, The Macmillan Press Ltd, Hampshire

Davis, B, (2003), The Net Comes Home, The New Scientist, 15th February 2003, p26-29,

Davis, F., Bagozzi, R.P and Warshare, P.R (1989), User acceptance of computer technology. A comparison of two theoretical models, Management Science, 35, 982-1003

Deng, M., Fritsch, L., Kursawe, K., (2006) Personal Rights Management - Taming camera-phones for individual privacy enforcement. LECT NOTES COMPUT SC 4258: 172-189 2006

Department of Health, (2007), The National Cancer Registry, http://www.dh.gov.uk/en/Policyandguidance/Healthandsocialcaretopics/Cancer/DH_4068586, date accessed 13 Dec 2007

Devitt,K and Roker, D, (2006), The Role of Mobile Phones in Family Communication, TSA, Brighton

DfES, 2007, About Contact Point - Every Child Matters, http://www.everychildmatters.gov.uk/deliveringservices/contactpoint/about/

Dinev, T. and Hart, P, (2004), Internet Privacy Concerns and their Antecedents - Measurement Validity and a Regression Model, Behaviour and Information Technology, Volume 23, Issue 6, November 2004 pages 413-422

Ding, C.H., and Buyya, R, (2004), Guided Google A Meta Search Engine and its Implementation, International Journal of Computers and Applications, Vol 26, Issue 3, p1465, www.gridbus.org/papers/guidedgoogle.pdf

Direct Gov, (2007), DirectGovKids, http://kids.direct.gov.uk/

Dixon, P., 2006, Medical Identity Theft: The information crime that can kill you. World Privacy Forum, Spring 2006, http://www.worldprivacyforum.org/medicalidentitytheft.html

Dowty, T, (2003), Can IT really protection children?, Guardian, Thursday, November 27 http://society.guardian.co.uk/futureforpublicservices/comment/0,,1094506,00.html

Drive Diagnostics, (2006), The Safety Centre, http://www.drivediagnostics.com/site/index.asp?FileToLoad=SuccessStories/TMobile.html

Dumas, J (1999) Usability Testing Methods: Subjective Measures, Part II - Measuring Attitudes and Opinions. American Institutes for Research. http://www.upassoc.org/html/1999_archive/usability_testing_methods.html

Dutton, W.H and Shepherd, A., (2004), Confidence and Risk on the Internet, Foresight, Cyber Trust and Crime Prevention Project, http://www.foresight.gov.uk/Previous_Projects/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/Confidence_and_Risk_on_the_Internet/Confidence_and_Risk_on_the_Internet.html

DVLA, (2007), DVLA Online Vehicle Licensing, http://www.vehiclelicence.gov.uk/EvlPortalApp/?SKIN=directgov#

eGov Monitor, (2005), Info Commissioner criticises ID Cards Bill, The Register, 28th October 2005 http://go.theregister.com/feed/http://www.theregister.co.uk/2005/10/28/id_card_bill_concerns/

EPIC, (2007), Electronic Privacy Information Centre, Online Guide to Practical Privacy Tools, http://www.epic.org/privacy/tools.html

European Commission (EU), (2003), Data Protection, Eurobarometer, Special Eurobarometer, http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_highlights.pdf

European Commission, (2006), Safer Internet Programme, Europe's Information Society, http://europa.eu.int/information_society/activities/sip/index_en.htm

Evans, M, (2001), Model for Managing Information Flow on the World Wide Web, University of Plymouth, Plymouth,

Evening Standard, (2007), George Orwell, Big Brother is watching your home, Evening Standard, 28 April

2007, http://www.thisislondon.co.uk/news/article-23391081-details/George+Orwell,+Big+Brother+is+watching+your+house/article.do

Federrath, H, (2005), Privacy enhanced technologies: Methods - Markets - Misuse, Trust, Privacy, and Security in Digital Business, LNCS 3592: 1-9http://www-sec.uni-regensburg.de/publ/2005/Fed2005TrustBus05InvitedPaper.pdf

Feenberg, A, (1999), Questioning Technology, Routledge, London

Felson, M and Clarke, R.V., (1997), the ethics of situational crime prevention, in Newman, G., Clarke, R.V., and Shoham S.G. (Eds), Rational choice and Situational Crime Prevention: Theoretical Foundations, 197-217, Aldershot, Ashgate.

Ed:) Fensel, D. Hendler, J, Lieberman, H. Wahlster, W, (2003), Spinning the Semantic Web, The MIT Press, Cambridge, Massachusets,

Fidis, (2007), Future of Identity in the Information Society, http://www.fidis.net/

Field, T, (2006), Bullying by mobile phone and abusive text bullying, The Field Foundation, , http://www.bullyonline.org/schoolbully/mobile.htm

Fildes, J, (2006), Privacy worries over web's future, BBC, 24/05/2006, http://news.bbc.co.uk/1/hi/technology/5009774.stm

Finder, A., (2006), For Some, Online Persona Undermines a Resume, New York Times, 11 June 2006, http://www.nytimes.com/2006/06/11/us/11recruit.html?ex=1307678400&en=ddfbe1e3b386090b&ei=5090

Finkelhor, D., Mitchell, K. & Wolak, J. (2003). The exposure of youth to unwanted sexual material on the Internet: a national survey of risk, impact and prevention. Youth & Society, 34(3), 330–358.

Fiveash, K, (2006), Internet safety talks for UK kids, The Register, http://www.theregister.co.uk/2006/09/20/internet_children_safety/

Fox, W.M., (1995), Sociotechnical System Principles and Guidelines: Past and Present, Journal of Applied Behavioural Science, 3, 1995; Vol 31, pp91-105

Fraud Advisory Panel, 2006, 7th Annual Review, http://www.fraudadvisorypanel.org/cheker/cheker.php?idmk=31

Fraud Advisory Panel, (2007a), Government should extend legislation into virtual communities, fraudadvisorypanel.org, May 2007, http://www.fraudadvisorypanel.org/newsite/PDFs/pressreleases/Government%20Should%20Extend%20Legislation%20into%20Virtual%20World%20010507.pdf

Fraud Advisory Panel, (2007b), Missing an opportunity - Fraud review left high and dry, fraudadvisorypanel.org, March 2007, http://www.fraudadvisorypanel.org/newsite/PDFs/pressreleases/Missing%20an%20Opportunity%20Fraud%20Review%20150307.pdf

Fried, C., (1984), Privacy: A moral Analysis. in (Ed:) Schoeman, F.D, (1984), Philosophical Dimensions of Privacy, Cambridge University Press, Cambridge

Furedi, F, (2002), Culture of Fear, Continuum, London

Furnell, S, (2005), Internet threats to end-users: Hunting easy prey, Network Security, July, pp5-9

Galliers, R.D and Land F.F, (2002), Choosing Appropriate Information Systems Research Methodologies, In Qualitative Research in Information Systems, Myers, M.D., Avison, D. (Eds), Sage Publications Ltd, Gateshead,

Gallivan, M.J., and Keil, M, (2003), The user-developer communication process: a critical case study, Info Systems Journal, 13, pp37-68,

Gandon, F.L., Sadeh, N,M., (2004), Semantic Web Technologies to Reconcile Privacy and Context Awareness, Journal of Web Semantics, Volume 1, Issue 3http://www.websemanticsjournal.org/ps/pub/2004-17

Garfinkel, S, (2000), Database Nation, O'Reilly Associates, Sebastopol, CA

Garfinkel, S., Rosenberg, B., (Eds) (2006), RFID: Applications, Security and Privacy, Addison Wesley, USA.

Garland, D, (2000), Ideas, Institutions and Situational Crime Prevention. In Hirsch, A., Garland, D., Wakefield, A., (2000) (Eds) Ethical and Social Perspectives on Situational Crime Prevention, Hart, Oxford.

Gartner Group, (2005), Special Report: Technology, , http://www.gartner.com/research/special_reports/hype_cycle/hc_special_report_part1.jsp, last accessed December 2007

Gellman, R, (1997) Does Privacy Law Work? in Agre, P.E., and Rotenberg, M, (1997), (Eds) Technology and Privacy: The New Landscape, MIT Press, LondonDate Read : 01/11/2005

George, J.F, (Ed) (2004), Computers in Society: Privacy, Ethics and the Internet, Pearson Education Inc, New Jersey#

Get Safe Online, (2007), Get Safe Online, www.getsafeonline.org

Geiger, M., Cranor, L.F., (2005) counter-Forensic Privacy Tools. Institute for Software Research International School of Computer Science, Carnegie Mellon University, http://reports-archive.adm.cs.cmu.edu/anon/isri2005/abstracts/05-119.html

Gillham, B, (2000), Case Study Research Methods, Continuum, London

Gindin, S.E, (2000), Creating an Online Privacy Policy, www.info-law.com, February, 13, 2000 http://www.info-law.com/create.html

Glaser, B.G., Strauss, A.L., (1967), The discovery of grounded theory. Chicago. Aldine.

Goldberg, I., (2003) Privacy Enhancing Technologies for the Internet II: Five years later. LECT NOTES COMPUT SC 2482: 1-12 2003

Goo, S.K., (2006) Concerns raised over AT&T Privacy Policy, The washington Post, 23 June 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/22/AR2006062201742.html

Goodchild, S and Heathcote, E, (2005), I was getting 40 texts a day. Then they became really sinister, The Independent on Sunday, September 18, 2005

Google, (2007), About Gmail, http://mail.google.com/mail/help/intl/en/about.html#ads

Government of Alberta (GOA), (2003), Privacy Taxonomy, http://www.ipc.on.ca/index.asp?navid=46&fid1=387

Granger, S., (2001) Social Engineering Fundamentals, Part I: Hacker tactics., Security Focus,

www.securityfocus.com/print/infocus/1527

Granneman, S, (2003), RFID Chips are Here, Security Focus, www.securityfocus.com, http://www.securityfocus.com/columnists/169

Gray, K., (2007) How will your online profile affect potential job offers? JobWeb, http://www.jobweb.com/resources/library/Parents/How_Will_Your_O_302_1.htm

Gregor, S., (2006), The Nature of Theory in Information Systems, MIS Quarterly, vol. 30, no. 3, pp. 491-506, Sept. 2006.

GRO, (2007), General Register Office, http://www.gro.gov.uk/gro/content/ date accessed 27/04/07

Gruteser, M., Grunwald, D, (2003), A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks, , http://systems.cs.colorado.edu/Papers/Generated/2003wlanPrivacyAssessment.pdf

Guerra, A.G., Zizzo, D.J., Dutton, W.H and Peltu, M, (2003), Economics of Trust in the Information Economy: Issues of Identity, Privacy and Security, Oxford Internet Institute, Research Report No 1, April 2003. http://www.oii.ox.ac.uk/resources/publications/RR1.pdf

Guardian, (2006), Identity fraud 'affects one in ten', Guardian Unlimited, August 9th 2006 http://www.guardian.co.uk/money/2006/aug/09/business.scamsandfraud

Hansen, M., and Krasemann, H., (2005), Privacy and Identity Management for Europe, Prime Consortium, http://www.prime-project.eu.org/whitepaper/

Hannay, J.E.; Sjoberg, D.I.K.; Dyba, T., (2007), A Systematic Review of Theory Use in Software Engineering Experiments, IEEE Transactions on Software Engineering, Vol.33, Iss.2, Feb. 2007, Pages:87-107

Haralambos, M., Holborn, M., (1991), Sociology Themes and Perspectives, Collins Educational, London

Harper, S, (2006), Information Management Group, University of Manchester, , http://img.cs.man.ac.uk/research.shtml

Hawkey, K., Inkpen, K.M, (2006), Examining the Content and Privacy of Web Browsing Incidental Information, WWW2006, Scotlandhttp://www2006.org/programme/item.php?id=36

HBOS (2006) Children In London Are 2006's Pocket Money Winners, Halifax and Bank of Scotland, http://www.hbosplc.com/media/pressreleases/articles/halifax/2006-04-15-01.asp?fs=/media/press_releases.asp

Heath, C., Luff, P, (2000), Technology in Action, Cambridge University Press, Cambridge,

Herrigel, A., Jian, Z., (2006), RFID identity theft and countermeasures, OPTICAL SECURITY AND COUNTERFEIT DETERRENCE TECHNIQUES VI 6075: 7510-7510, 2006, in Renesse, R.L.V., (Ed) PROCEEDINGS OF THE SOCIETY OF PHOTO-OPTICAL INSTRUMENTATION ENGINEERS (SPIE).

Hewlett Packard, (2006), HP Labs Semantic Web Research, HP Development Company, Bristol, http://www.hpl.hp.com/semweb/hpl-research.htm

Hine, C., Eve, J., (1998), Privacy in the marketplace : Social construction of privacy, The Information society , vol. 14, no4, pp. 253-262

Hine, C, (2000), Virtual Ethnography, Sage Publications, London,

HiSPEC, (2002), "Privacy Enhancing Technologies State of the Art Review", www.hispec.org.uk,

http://www.hispec.org.uk/public_documents/7_1PETreview3.pdf (accessed 30 November 2006)

Hirsch, D. D, (2005), Is Privacy Regulation the Environmental Law of the Information Age?, Privacy and Technologies of Identity: A Cross Disciplinary Conversation, Strandburg, K and Raicu, D.S (Eds) Springerhttp://ssrn.com/abstract=799285

Hitwise, (2007), Hitwise ISP Partner Program, http://www.hitwise.co.uk/other/isp-fact-sheet.php

HMG, (2006), Information Sharing Vision Statement, HM Government, September 2006, http://www.dca.gov.uk/foi/sharing/information-sharing.pdf

Hochhauser, M, (2000), Why I stopped shopping at Amazon.com: A Reading Expert Sounds Off, Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/amazon.htm

Hof, R., (2006), My Virtual Life, Business Week, http://www.businessweek.com/magazine/content/06_18/b3982001.htm

Home Office, (2006), Situational Crime Prevention (SCP), www.crimereduction.homeoffice.gov.uk/learningzone/scp.htm

Home Office, (2007), The Identity and Passport Service, http://www.passport.gov.uk/index.asp

HOSDB, (2007), Home Office Scientific Development Branch, http://scienceandresearch.homeoffice.gov.uk/hosdb/about-us/

Howard, R., (2007), Concern over new fraud reporting, BBC Radio 4 Money Box, 31 March 2007, http://news.bbc.co.uk/1/hi/programmes/moneybox/6513835.stm

Howe, HL., Lake, AJ., Shen, T, (2007), Method to assess identifiability in electronic data files, American Journal of Epidemiology, 165 (5): 597-601 MAR 1 2007

Hudson, W, (2002), The Objective Web, ACM SIGCHI Bulletin , Volume 34, July-August 2002, http://www.syntagm.co.uk/design/articles/objweb.htm

Hughes, D.M., (2003), Prostitution online, Journal of Trauma Practice, Vol 2. No 3/4, 2003, pp115-132 http://www.uri.edu/artsci/wms/hughes/internet.pdf

Insafe, (2007), Insafe Network, www.safeterinternet.org

Introna, L, (2005), Phenomenological Approaches to Ethics and Information Technology, Metaphysics Research Lab, Stanford University, http://plato.stanford.edu/entries/ethics-it-phenomenology/#2

Jackson, J., Allum, N., Gaskell, G, (2004), Perceptions of risk in Cyberspace, Cyber Trust and Crime Prevention Project, , http://www.dti.gov.uk/files/file15284.pdf

James Moor, 2000, Towards a theory of privacy for the information age. In RM Baird, R Ramsower and S E Rosenbaum eds: Cyberethics, Moral, social and legal issues in the computer age. Amhurst, New York, Promethus books, pp 200-212

Jarvinen, O.P., Earp, J.B., Anton, A.I., (2002), Visibility Classification Scheme for Privacy Management Requirements, 2nd Symposium on Requirements Engineering for Information Security, (SREIS)

Jary, D., Jary, J, (1995), Dictionary of Sociology, Harper Collins, Glasgow

Jenkins, S., (2007) The British media does not do responsibility. It does stories. The Guardian, 18 May 2007. http://www.guardian.co.uk/commentisfree/story/0,,2082507,00.html

Johnston, (2007), Mind how you walk. It could be a crime. Telegraph. 26 March 2007, http://www.telegraph.co.uk/opinion/main.jhtml?xml=/opinion/2007/03/26/do2602.xml

Jones, S, (1999), (Ed) Doing Internet Research, Sage, London

Jutla, D., Bodorik, P., Gao, D, (2004), Management of Private Data: Addressing user Privacy and Economic, Social and Ethical Concerns, In LNCS 3178, Secure Data Management, pp100-117, Springer Verlag, Berlin

Jutla, D.N., Bodorik, P, (2005), Sociotechnical Architecture for Online Privacy, IEEE Security and Privacy, March/April 2005, pp29 - 39

Kelly, L., (2007), Phishing attacks get personal, Web User, 9 February 2007, http://www.webuser.co.uk/news/news.php?id=109309

Ed: Kemshall, K., McIvor, G, (2004), Managing Sex Offender Risk, Research Highlights in Social Work 46, Aberdeen

Kent, R., (2001), Data construction and data analysis for survey research. Palgrave, Hampshire.

Kerner, S.M, (2005), Consumers Want Personalization -- and Privacy, ClickZStats Security Issues, August 16, 2005, http://www.clickz.com/stats/sectors/security/article.php/3527716

Kim, A., Hoffman, L, J., Martin, C,D.,, (2002), Building Privacy into the Semantic Web: An Ontology Needed Now, In Proceedings of Semantic Web Workshop WWW 2002, http://semanticweb2002.aifb.uni-karlsruhe.de/proceedings/Position/kim2.pdf

Kirda, E., Kruegel, C., (2006), Protecting users against phishing attacks, COMPUTER JOURNAL 49 (5): 554-561 2006

Kirk, J., (2007), Update: Security Expert cracks RFID chip in UK passport, InfoWorld, 6 March 2007, http://www.infoworld.com/article/07/03/06/HNexpertcracksrfidchip_1.html

Kiss, J., (2007), Most teens are MySpacers, Media Guardian, 17 May 2007, http://www.guardian.co.uk/media/2007/may/17/digitalmedia.socialnetworking

Kjaerland, M, (2006), A taxonomy and comparison of computer security incidents from the commercial and government sectors, Computers & Security, Vol 25, Issue 7, pp522-538,

Kluth, A, (2004), Make it Simple, The Economist, 28th October 2004, Online Edition,

Kobielus, J., (2007), Mastering Customer Records, CRM Magazine, Dec 2007, Vol 11, Issue 12, p48

Koivunen, M and Miller, E, (2001), W3C Semantic Web Activity, In proceedings of Semantic Web Kick-off Seminar, Finland Nov 2, 2001, http://www.w3.org/2001/12/semweb-fin/w3csw

Kolari, P., Ding, L., Ganjugunte, S., Kagal, L., Joshi, A., and Finin T, (2005), UMBC eBiquity Publication: Enhancing Web Privacy Protection through Declarative Policies, Proceedings of the IEEE Workshop on Policy for Distributed Systems and Networks(POLICY 2005), June 07, 2005, http://ebiquity.umbc.edu/paper/html/id/213/

Kunzru, H., (2007) Host not found, The Guardian, 31 March 2007, http://books.guardian.co.uk/departments/politicsphilosophyandsociety/story/0,,2046857,00.html

Lacohee, H., Crane, S., Phippen, A., (2006), Trustguide: Final report. http://www.trustguide.org.uk/publications.htm

Lager, M., (2007), Simple Truth about Complex Manufacturing, CRM Magazine, Nov 2007, Vol 11, Issue 11, p14-15

Lahlou, S., Langheinrich, M., Rocker, C., (2005), Privacy and trust issues with invisible computers, In Communications of the ACM, Vol 48, Issue 3, March 2005, pp59-60

Lanchester, J., (2006), A bigger bang., The Guardian, Saturday 4th November 2006.

Land Registry, (2007), Land Registry, http://www.landregistry.gov.uk/ date accessed 27/04/07

Langheinrich, M., (2002), Privacy Invasions in Ubiquitous Computing, Ubicomp Privacy Workshop.

Larose, R., Rifon, NJ, (2007), Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior, Journal of Consumer Affairs, 41 (1): 127-149 SUM 2007

Lauesen, S, (2005) User Interface Design, Addison-Wesley, Harlow.

Lee, R, (2002), Personal Data Protection In the Semantic Web , W3C, http://www.w3.org/2002/01/pedal/thesis.html

Lee, S,M., Lee, Z., Lee, J., (2007), Knowledge transfer in work practice: adoption and use of integrated information systems, INDUSTRIAL MANAGEMENT & DATA SYSTEMS 107 (3-4): 501-518

Lee, J., Kim, J., (2007), Grounded theory analysis of e-government initiatives: Exploring perceptions of government authorities, GOVERNMENT INFORMATION QUARTERLY 24 (1): 135-147 JAN 2007

Leenes, R. E., Koops, B.J., (2005), Code' and Privacy - Or How Technology is Slowly Eroding Privacy, Essays on the Normative Role of Information Technology, T.M.C. Asser Press, The Hague

Lefley, F, (1997), Approaches to risk and uncertainty in the appraisal of new technology capital projects, International Journal of Production Economics, Volume 53, Issue 1, 6 November 1997, Pages 21-33

Lehrer, JA., Pantell, R., Tebb, K., Shafer, MA, (2007), Forgone health care among US adolescents: Associations between risk characteristics and confidentiality concern, Journal of Adolescent Health, 40 (3): 218-226 MAR 2007

Leigh, D., Evans, R., (2006), Illegal Investigators, a detective agency, and a leading law firm., The Guardian, 15 November 2006.Leigh, D., Evans, R., (2006), Illegal Investigators, a detective agency, and a leading law firm., The Guardian, 15 November 2006.

Lenhart, A., Madden, M, (2005), Teen Content Creators and Consumers, Pew Interent & American Life Project, Washingtonhttp://www.pewinternet.org/pdfs/PIP_Teens_Content_Creation.pdf

Lev-Ram, M., (2006) Ohmigod, teens are so over e-mail, Business 2.0 Magazine, 26 July 2006, http://money.cnn.com/2006/07/26/technology/thirdscreen0726.biz2/index.html

Lewin, K., (1946), Action Research and Minority Problems. Journal of Social Issues. 2(4): 34-46

Lewis, P., (2006) Teen Network websites face anti-paedophile investigation. The Guardian, 3 July 2006.

Li, Q., (2007), New bottle but old wine: A research of cyberbullying in schools. In Computers in Human Behaviour, Volume 23, Issue 4, (July 2007), p1777-1791.

Likert, R., (1932) A Technique for the Measurement of Attitudes. Archives of Psychology 140, pp1-55

Lindblom, C.E., (1987), Alternatives to Validity: Some Thoughts Suggested by Campbell's Guidelines. Knowledge Creation, Diffusion, Utilization, vol. 8, pp. 509-520, 1987.

Livingstone, S, (2003), Children's use of the internet: reflections on the emerging research agenda, In New Media & Society, 5 (2), p147-166, Sage

Livingstone, S., Bober, M, (2005), UK Children Go Online, LSE, http://personal.lse.ac.uk/bober/UKCGOfinalReport.pdf

Lynch, M.D., (1997), The Use of Soft Systems Methodology in Multi-Voiced Groups, In Proceedings of EIASM conference in Leuven, Belgium, http://www.cems.uwe.ac.uk/~mlynch/Papers+OtherWritings/SSMInMulti-VoicedGroups/SSMInMulti-VoicedGroups.html

McMillan, S.J. and Morrison, M, (2006), Coming of age with the Internet, In New Media & Society, Vol 8 (1), PP 73-95, Sage, London

Magid, L, (2004), Teen Safety on the Information Highway, National Center for Missing and Exploited Children, http://www.safeteens.com/safeteens.htm#Guidelines_for_Parents_0

Margulis, S.T, (1977), Conceptions of Privacy: Current Status and Next Steps, In Journal of Social Issues, 33. 5-10

Markovsky, B., (1994), The Structure of Theories. Foschi, M., and Lawler, E.J., (Eds.), Group Processes, pp. 3-24, Nelson-Hall, 1994.

Martin, D., (2005) Privacy Analysis for the Casual User with Bugnosis. In Cranor, L.F., and Garfinkel, S., (Eds) Security and Usability: Designing Secure Systems that People Can Use.

Massey, R., (2005) The dashboard spy keeping an eye on teenage drivers, The Dail Mail, 9 September 2005

May, T., (1993) Social Research: Issues, Methods and Process. Open University Press, Buckingham.

MSDN, (2007), Creating custom explorer bars, toolbars and deskbands, http://msdn2.microsoft.com/en-gb/library/aa969320.aspx

MSDN, (2007a), Windows Live Developer Centre, http://msdn2.microsoft.com/en-gb/live/default.aspx

Melly, T., (2007), Truths, half-truths and Wikipedia, The Register, 15th March 2007, http://www.theregister.co.uk/2007/03/15/tom_melly_wikipedia_comment/

Merrill, D., (2006), Mashups: The new breed of Web app, IBM, http://www-128.ibm.com/developerworks/xml/library/x-mashups.html

Metrics 2.0, (2007), Gartner says 80% of Active Internet Users Will have a Second Life, Metrics 2.0, 30 April, 2007, http://www.metrics2.com/blog/2007/04/30/gartner_says_80_of_active_internet_users_will_have.html

Mingers, J., (2001), Combining IS Research Methods: Towards a Pluralist Methodology. Information Systems Research. Sep 2001., Vol 12, Issue 3., p240.

Miller, H and Arnold J, (2001), Breaking Away from Grounded Identity? Women Academics on the Web, Cyberpsychology and Behaviour, Volume 4, Issue 1, 2001 Pages 95-108

Miller, E, (2005), Semantic Web Activity Statement, W3C, , http://www.w3.org/2001/sw/Activity

Ministry of Justice (MOJ), (2007), Anonymous registration for electors protects vulnerable,

http://www.gnn.gov.uk/content/detail.asp?ReleaseID=287898&NewsAreaID=2&NavigatedFromSearch=True

Minnesota Program Development, Inc, (2006), Power and Control Wheel, www.duluth-model.org, Minnesota http://www.duluth-model.org/documents/PhyVio.pdf

Mitchell KJ, Finkelhor D, Wolak J, (2005), The Internet and family and acquaintance sexual abuse, Child Maltreatment, 10 (1): 49-60 FEB 2005

Mitchell, K., Wolak J., and Finkelhor, D. (2007), Trends in youth reports of sexual solicitations, harassment and unwanted exposure to pornography on the Internet, J Adolesc Health 40 (2007), pp. 116–126.

Mitnick, K.D., Simon, W.L., and Simon, W., (2002), The Art of Deception: Controlling the Human Element of Security, John Wiley & Sons, Inc. New York, NY, USA

Mulholland, H., (2007) Privacy Tsar warns over data losses. Guardian Unlimited, 24th December 2007, http://politics.guardian.co.uk/publicservices/story/0,,2232094,00.html?gusrc=rss&feed=networkfront

Mullen, P.E., (2006) Assessing and managing the risks in the stalking situation, Journal American Academy PSYCHIATRY 34 (4): 439-450 2006

Mumford, E, (2003), Redesigning Human Systems, IRM Press, London

Muncaster, P., (2006), Semantic Web threatens data privacy, IT Week, 13/06/06, http://www.itweek.co.uk/itweek/news/2158160/semantic-web-threatens-privacy

Myers, M.D., and Avison, D., (2002) (Eds) Qualitative Research in Information Systems. Sage. London

NCH, (2007), Internet Safety, http://www.nch.org.uk/information/index.php?i=209

Nelson, R, (1998), Privacy Evaluator, W3C, http://www.w3.org/Privacy/19981101-evaluator.html

Newman, G.R., McNally, M.M., (2005), Identity Theft Literature Review, NCJRS, www.ncjrs.org/pdffiles1/nij/grants/210459.pdf, date accessed December 2007

Nielsen, (2006), The Ages of the Internet, http://www.netratings.com/pr/PR_060306_UK.pdf

Nielsen, (2007), Time shows eBay and RuneScape to be the UK's Most Engaging Sites, 17 April 2007, http://www.netratings.com/pr/pr_070417_UK.pdf

No2ID, (2007), Stop ID Cards and the database state, http://www.no2id.net/

Noguchi, Y, (2006), In teens web world My Space is s last year. Washington Post, 29 October 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/10/28/AR2006102800803.html

NSPCC, (2007), Help and advice for parents and carers, http://www.nspcc.org.uk/helpandadvice/parentsandcarers/helpandadviceforparentsandcarers_wda38727.html

Nuseibeh, B. and Easterbrook, S. (2000) 'Requirements Engineering: A Roadmap', in The Future of Software Engineering, editor Finkelstein, A. ACM, New York, pp. 35-46.

O2, (2006), LookAtMe, O2, http://www.o2.co.uk/fungames/lookatme

OASys, (2002), Offender Assessment System: User Manual V2, Crown Copyright.

Oates, J, (2004), Tesco Extends RFID chip roll-out, The Register, 27, September, 2004

http://www.theregister.co.uk/2004/09/27/tesco_rfid_rollout/

Oates, J., (2006), DVLA makes £6.5m selling addresses, The Register, 19th June 2006, http://www.theregister.co.uk/2006/06/19/dvla_sells_you_down_river/

O'Brien, C, (2006), BoI customers fall victim to phishing scam, The Register, 17 August 2006, http://www.theregister.co.uk/2006/08/17/boi_phishing_attack/

O'Connell, R., Bryce, J., (2006), Young People, Well Being and Risk Online, Council Of Europe, , http://www.coe.int/t/e/human_rights/media/1_Intergovernmental_Co-operation/MC-S-IS/H-inf(2006)005_en.pdf

Öhman Persson, J., (2004), The Obvious & The Essential: Interpreting Software Development & Organizational Change, Thesis, Uppsala University.

OJR, (2006), Blog Software comparison chart, Online Journalism Review, The Annenberg Center for Communication at USC, 18 May 2006, http://www.ojr.org/ojr/images/blog_software_comparison.cfm

Office of Management and Budget (OMB) (2003), OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M -03-22, Memorandum for Heads of Executive Departments and Agencies, Office of Management and Budget, The Executive Office of the President, Washington, DC.

ONS, (2002), National Statistics Socio-economic Classification, http://www.statistics.gov.uk/methods_quality/ns_sec/continuity.asp

Oppliger, R, (2005), Privacy-enhancing technologies for the world wide web , Computer Communications, 28 (16) Pages 1791-1797

O'Reilly, T., (2005), What is Web 2.0, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html

Outlaw, (2003), Court refuses 192.com access to full electoral register, http://www.out-law.com/page-3865

Page, L., (2007), Judge in tech trial says he 'doesn't know what a website is', The Register, 17 May 2007, http://www.theregister.co.uk/2007/05/17/judge_website_shocker/

Palm, E., Hansson, S.O., (2006), The case for ethical technology assessment (eTA), Technological Forecasting and Social Change, Volume 73, Issue 5, June 2006, Pages 543-558

Passin, T.B, (2005), Explorers guide to the semantic web, Manning, Greenwich, USA

Patrick, AS, Kenny, S (2003) From privacy legislation to interface design: Implementing information privacy in human-computer interactions, LECT NOTES COMPUT SC 2760: 107-124 2003

PC Magazine, (2007), Top 10 Security Threats, PC Magazine, April 2007, Vol 26, Issue 7/8, p66-67

Physorg news, (2005), Anti-Theft RFID Clothing, United Press International, August 01 http://www.physorg.com/news5537.html

Plant, S., (2000). On the mobile: the effects of mobile telephones on social and individual life, http://www.motorola.com/mot/doc/0/234_MotDoc.pdf

Power, M, (2006), How to catch a cheating partner, The Independent, 17th February, 2006

Preece, J. et al, (1994), Human Computer Action, Pearson Education, Harlow

Prensky M (2005) What Can You Learn from a Cell Phone? Almost Anything! Innovate 1 (5). http://www.elearningsource.info/elearning/What%2520Can%2520You%2520Learn%2520from%2520a%2520Cell%2520Phone.pdf

Prime, (2007), Privacy and Identity Management for Europe, https://www.prime-project.eu/

Privacy Bird, (2005), Privacy Bird, , http://www.privacybird.org/

Privacy Fox, (2007), Privacy Fox, http://privacyfox.mozdev.org/

Quinn, M.J, (2005), Ethics for the Information Age, Pearson Education Inc, USA

Raab, C.D and Bennett, C.J, (1998), Distribution of Privacy Risks: Who Needs Protection, Information Society, Vol 14, Issue 4, p 263-274

Raab, C. (2003), 'Privacy Impact Assessment: The Question of Risk', paper presented to the International Workshop on Privacy Impact Assessment, Office of the Privacy Commissioner, Auckland, NZ, 16 Sept.

Raab, C.D., (2004), The Future of Privacy Protection, Cyber Trust and Crime Prevention Project, http://www.foresight.gov.uk/Previous_Projects/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/The_Future_of_Privacy_Protection/The_Future_of_Privacy_Protection.html

Reid, M., (2007), Think before you drive boy racers off the road, The Times, 30 April 2007, http://www.timesonline.co.uk/tol/comment/columnists/guest_contributors/article1722944.ece

Richards, N. M. and Solove, D. J., (2007), Privacy's Other Path: Recovering the Law of Confidentiality, Georgetown Law Journal

Rickert, V., Ryan, O., (2007), Is the Internet the Source?. Journal of Adolescent Health, Volume 40, Issue 2, Pages 104-105

Rightmove.co.uk, (2007), http://www.rightmove.co.uk/template/publicsite,aboutus,AVM.vm#wdta, date accessed 19/04/2007

Roberts, G, (2005), RFID and What It Promises For The Retail Industry , Retail Solutions 2005, http://www.retailsolutions2005.co.uk/2005/news_roberts.html

Rootsecure, (2006), Locate almost anyone in the UK without their permission, rootsecure.net, retrieved February 2006 http://www.rootsecure.net/?p=reports/locate_anyone_in_uk

Ronkko, K., 2002, Software Practice from the Inside: Ethnography Applied to Software Engineering, Thesis, Blekinge Institute of Technology.

Royal Academy of Engineering (RAE), (2007), Dilemmas of Privacy and Surveillance, Royal Academy of Engineering report, http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf

Rubens, P., (2007), How to keep your wi-fi network safe, BBC, http://news.bbc.co.uk/1/hi/technology/6595703.stm

Russell, C, (2005), Appraisal of Safe Harbour Arrangements, www.charlesrussell.co.uk, http://www.cr-law.co.uk/articles/viewarticle.asp?articleid=915

Safer Motoring, (2006), Newly qualified and Teenage Drivers, http://www.safermotoring.co.uk/NewlyQualifiedTeenageDrivers.html

Samarajiva, R, (1997), As Though Privacy Mattered. In Ed: Agre, P.E., and Rotenberg, M, (1997), Technology and Privacy: The New Landscape, MIT Press, London

Sanders, E., (2002), Ethnography in NPD research. How "applied ethnography"can improve your NPD research access, PDMA, www.pdma.org/visions/apr02/applied.html

Saunders, H., Barron, J., (2003), Failure to Protect?. Women's Aid, Bristol.

Schwartz, P. M., (1999), Privacy and Democracy in Cyberspace, Social Science Research Network, http://www.paulschwartz.net/pdf/VAND-SCHWARTZ.pdf

Searle, R.H., (2006), New technology: the potential impact of surveillance techniques in recruitment practices, In Personnel Review, 2006, Volume 35 Issue 3 Page: 336 - 351, Emerald Group Publishing Limited

Security Views, (2006), Medical Identity Theft, In Computers and Security, Vol 25 (6), P402.

Seymour, R., (2002). Surprise Me. Design Council, London

Shallcross, B, (2006), Teddy phone - safe or sorry?, Shallcross, B, Tuesday, 14th March 2006, Westminster Blog. http://web.mac.com/brianshallcross/iWeb/Site/Brian%20Shallcross%20at%20Westminster/47E95D35-0894-445C-A857-8A6998A82408.html

Shepard, M, (2005), Twenty Years of Progress in Addressing Domestic Violence, Journal of Interpersonal Violence, Vol 20, No 4, April 2005, 436-441

Shneiderman, B., Plaisant, C., (2005), Designing the User Interface. Pearson Education.

Simmons, D., (2007), Keeping secrets from web spies, BBC 9 February 2007, http://news.bbc.co.uk/1/hi/programmes/click_online/6345629.stm

Sinclaire, J.K., Wilkes, R.B, Simon, J.C., (2006), Internet transactions: perceptions of personal risk, International Journal of Networking and Virtual Organisations, Volume 3, Number 4, 28 December 2006, pp. 425-437(13)

Simon, R, Frohlich, P, Hanegg, H,.(2006), Beyond location based - The spatially aware mobile phone, WEB AND WIRELESS GEOGRAPHICAL INFORMATION SYSTEMS, PROCEEDINGS 4295: 12-21, 2006

Slashdot, (2007), ISPs may be selling your web clicks. http://slashdot.org/articles/07/03/16/1958211.shtml

Smart Card Group, (2006), ICAMCU , , http://www.icamcu.com/

Smith, T, (2003), Nokia Observation: camera phone or CCTV?, The Register, http://www.theregister.co.uk/2003/06/12/nokia_observation_camera_phone/

Solove, D.J, (2003), Identity Theft, Privacy, and the Architecture of Vulnerability, Hastings Law Journal, Vol 54 1227, 1232

Solove, D.J, (2004), The Digital Person, New York University Press, New York

Solove, D, (2006), A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol 154, No 3, p477

Sommerville, I, (2001), Software Engineering. 6th Ed., Pearson Education Ltd, Harlow,

Sophos, (2007), Security Threat Report 2007, Sophos, http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threats-2007_wsrus.pdf,

accessed December 2007

Southworth, C., Dawson, S., Fraser, C., Tucker, S., (2005), A High Tech Twist on Abuse: Technology, Intimate Partner Stalking and Advocacy, Violence Against Women Online Resources, Minesota http://www.mincava.umn.edu/documents/commissioned/stalkingandtech/stalkingandtech.html

Spitzberg, B.H., Hoobler, G, (2002), Cyberstalking and the Technologies of Interpersonal Terrorism, New Media & Society, Vol 4, No 1, pp71-92, March 2002

Stahal, B.C., (2004) Responsibility for Information Assurance and Privacy: A problem of individual ethics? In Journal of Organisational and End User Computing, Jul-Sep 2004, Vol 16, Issue 3, p59-77

Stalder, F, (2002), The Voiding of privacy, Sociological Research Online, 7 (2): - Aug 31 2002

Starks, H., Trinidad, S.B., (2007), Choose your Method: A Comparison of Phenomenology, Discourse Analysis, and Grounded Theory. Qualitative Health Research, 12, 2007; Vol 17, pp 1372 – 1380

Stevens, T., (2007), Identity, Identity, Identity. BCS Enterprise Security, http://www.bcs.org/server.php?show=ConWebDoc.11113

Strauss, A., Corbin, J., (1998), Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, Sage, London

Suchman, L.A., (1991), Plans and Situated Actions, Cambridge University Press, Cambridge

Suffolk, (2006), Interlocking Steps to Success, PITCOM briefing, http://www.pitcom.org.uk/briefings/CIO-Nov06.pdf.

Sullivan, D., (2006), Nielsen NetRatings Search Engine Ratings, http://searchenginewatch.com/showPage.html?page=2156451

Sweeney, L., (2006) Protecting Job Seekers from Identity Theft. IEEE Internet Computing 10 (2) March 2006. http://privacy.cs.cmu.edu/dataprivacy/projects/idangel/idangel3.pdf

Symantec, (2007), Symantec Internet Threat Security Report: Trends for January to June 2007, Symantec, September 2007, http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007.en-us.pdf, accessed December 2007

Tauberer, J., (2006) Semantic Web/RDF Library for C#/.NET. http://razor.occams.info/code/semweb/

Tavani, H.T, (2007), Ethics and Technology 2nd Edition, Wiley, USA

TechDirt, (2007), Is your ISP selling your clickstream data? Do you have any privacy at all? http://www.techdirt.com/articles/20070313/213014.shtml

Technology Quarterly, (2006), Tracking Your Every Move, The Economist, December 2nd, 2006 p11-12

Tedeschi, R., (2006) E-Commerce Report: Online swindlers shift focus to smaller retailers, New York Times, 11 December 2006, http://query.nytimes.com/gst/fullpage.html?res=9406E7DB1431F932A25751C1A9609C8B63

Tendler, S, (2005), Nationwide spy system to track millions of car journeys a day, The Times, 23 December 2005, http://www.timesonline.co.uk/tol/news/article782165.ece

The Big Opt Out, (2006), NHS Confidentiality Campaign, http://www.nhsconfidentiality.org/?page_id=3

Thomson, I, (2005), Identity Theft - the facts, ComputerActive, 17 June 2005 www.computeractive.co.uk/computeractive/features/2138242/identity-theft-facts

Trafficmaster, (2007), Traffic Master, http://www.trafficmaster.co.uk/index.html

Treese, W, (2006), Web 2.0: Is it really different?, netWorker, Vol 10, No 2, pp 15-17

Tomlinson, H., and Evans, R., (2005), Tesco stocks up on inside knowledge of shoppers lives, The Guardian, 20th September 2005, http://business.guardian.co.uk/story/0,3604,1573821,00.html date accessed 20/04/07

Tynan, D, (2005), Computer Privacy Annoyances, O'Reilly, USA

Updegrove, A, (2005), A New Vision From the Inventor of the World Wide Web: An Interview With Tim Berners-Lee, MarketingProfs.Com, August 2, 2005 http://www.marketingprofs.com/5/updegrove1.asp

Valongo, K, (2000), Your Privacy on the Internet, Internet Handbooks, Plymouth

Vence, D.L., (2007) CRM: You know what it stands for, but you may not know what it means. Marketing News, 15th September, 2007, Vol 41, Issue 15, p12

von Solms, B., (2006) Information security - The Fourth Wave, COMPUTERS & SECURITY 25 (3): 165-168 MAY 2006

W3C, (2004), RDF Specification, , , #http://www.w3.org/RDF#

W3C, (2006), Platform for Privacy Preferences (P3P) project, http://www.w3.org/P3P/

Wagner, S, (2005), Mobile HCI 2004: Experience and Reflection, IEEE Pervasive Computing, January-March 2005, Vol 4, Num 1, pp88-91,

Wainwright, M., (2007) Talking CCTV Cameras accuse the wrong person. The Guardian, 12 April 2007, http://society.guardian.co.uk/crimeandpunishment/story/0,,2055057,00.html

Waller, A.A., (2005), Work in progress - feminist research methodologies: why, what, and how. Frontiers in Education, 2005. FIE '05. Proceedings 35th Annual Conference, Vol., Iss., 19-22 Oct. 2005, Pages: F4H- 20-22

Ward, M, (2006), Wi-fi set to re-wire social rules, BBC, 8th March 2006http://news.bbc.co.uk/1/hi/technology/4770188.stm

Warren, S and Brandeis, L, (1890), The Right to Privacy, Quoted in Developing Key Privacy Rights, Colvin, M., Harvard Law Review, 4 (1890), 193

Warren, P, (2005), Mobile phones turned into point'n'buy devices , The Inquirer, 20th January 2005, http://www.theinquirer.net/?article=20827

Web Application Security Consortium, (2007), Web Hacking Incidents Database , http://www.webappsec.org/projects/whid/byyear_year_2007.shtml, accessed December 2007

Weick, K.E., (1989), Theory Construction as Disciplined Imagination, Academy of Management Rev., vol. 14, no. 4, pp. 516-531, 1989.

Westin, A. F., (2003), Social and Political Dimensions of Privacy, Journal of Social Issues, Vol 59, Issue 2, pp 431-453

Windley, P, (2005), Digital Identity, O'Reilly, USA

Winkelman, W.J., Leonard, K.J., Rossos, P.G., (2005) Patient-Perceived Usefulness of Online Electronic Medical Records: Employing Grounded Theory in the Development of Information and Communication Technologies for Use by Patients Living with Chronic Illness, Journal of American Medical Informatics Association, 2005;12:306-314

Wired News, (2006), Teens Reveal Too Much Online, Associated Press, 5th February, 2006, http://www.wired.com/news/wireservice/1,70163-0.html, date accessed 31/01/07

Wired, (2007) Does your ISP sell your internet history? Help 27B Investigate. http://blog.wired.com/27bstroke6/2007/03/does_your_isp_s.html

Womens Aid Federation of England (WAFE), (2002), Domestic Violence Statistical Factsheet 2002, , http://www.womensaid.org.uk/dv/dvfactsh2002.htm

Wood, R., Atkinson, S., Johnson, C., Phippen, A. (2007) Mobile phones and schools; the development of a taxonomy of risk, In Proceedings of World Conference on E-Learning in Corporate, Government, Healthcare and Higher Education, Canada

Working to Halt Online Abuse (WHOA), (2005), Online Harassment Statistics Harrasment pattern for 2000 - 2004, WHOA, http://www.haltabuse.org/resources/stats/pattern.shtml

World Telecommunication/ICT Development Report (2006) Measuring ICT for social and economic development (eighth edition), International Communications Union

Wu, Z., Chen, H.,Xu, J, (2003), Knowledge base grid: A generic grid architecture for semantic web, In Journal of Computer Science and Technology, v 18, n 4, July, 2003, p 462-473,

Yao, Mz., Rice, R.E., Wallis, K., (2007), Predicting user concerns about online privacy. In Journal of the American Society for Information Science and Technology, vol 58, no 5, (2007) pp710-722

Ybarra, M., Leaf, P. & Diener-West, M. (2004). Sex differences in youth-reported depressive symptomatology and unwanted Internet sexual solicitation. Journal of Medical Internet Research, 6(1), e5. http://www.jmir.org/2004/1/e5/.

Ybarra, M.L., (2006), Examining characteristics and associated distress related to Internet harassment: Findings from the Second Youth Internet Safety Survey, PEDIATRICS 118 (4): E1169-E1177 OCT 2006

Yearnshire, S., (1997), Analysis of Cohort, in Bewley, S., Friend, J., and Mezey, G., (Eds) Violence Against Women, London, RCOG.

Yin, R.K, (1994), Case Study Research Design and Methods, Sage Publications, London

Yin, R.K, (2003), Applications of case study research, Sage Publications, London

Yllo, K.A., (1993), Through a feminst lens: Gender, Power and Violence, in Gelles, R.J., and Loseke, D.R., (Eds) current controversies on family violence, p47-62, Sage Publications, Newbury Park.

Zeps, N., Iacopetta, BJ., Schofield, L., George, JM., Goldblatt, J, (2007), Waiver of individual patient consent in research: when do potential benefits to the community outweigh private rights?, Medical Journal of Australia, 186 (2): 88-90 JAN 15 2007

Zetter, K, (2004), Security Cavities Ail Bluetooth, Wired News, 8th August 2004http://wired.com/news/privacy/0,1848,64463,00.html?tw=wn_story_page_prev2

12 Appendix A – Questionnaires

12.1 Pre-Search Questions – Individuals not IT experts

Preliminary Interview for Personal Information Survey

Gender:
Age:
Profession:
Internet Proficiency Rating

How much information do you think is available about yourself over the Internet?

Do you have any concerns about this?

If so, what are they?

Do you consider there are any risks posed to yourself from that information accessible through the Internet?

If so, what?

12.2 Post-Survey Questions – Individuals not IT experts

Post Survey Interview for Personal Information Survey

Respondent Number:

How accurate do you think the information is?

Do you have any concerns about this?

If so, what are they?

Were you surprised in any way at the information found?

Do you consider there are any risks posed to yourself from that information accessible through the Internet?

If so, what?

12.3 Pre-Group Questionnaire – Focus groups

These questions are designed to help you focus on the topic we shall be discussing during this session. Please hand this to me at the end of the session as it will contribute to the analysis. Please circle all those that apply to you.

Gender Male Female

Age

Please list below how you make use of the Internet.

Do you use Instant Messaging? Yes No

Do you use a blog? Yes No
If yes, which one?

Do you use the Internet frequently to communicate with your friends?
Yes No

Have you signed up to websites that ask you personal information to register. For example: name, email address, age, date of birth, location, likes or dislikes.
Yes No
If yes, please list them here.

Are you worried in any way about how much personal information you have given to these websites?
Yes No

12.4 Focus group questions

Questions:

Please consider the following scenarios:

Your friends communicate with each other using a certain website – they invite you to join them. It involves you giving information about your birthday, your likes, dislikes, uploading a photo and giving your location.

What do you think about when answering these questions?

Do you mind giving the answers?

Does it worry you to give out this information?

Do you remember what you've said and where?

- This website that you have signed up to allows friends of your friends to see your details.
  - Does this worry you?
  - How might you control who sees or finds out what about you?

3. Have you any bad experiences with people contacting you through the Internet?

4. Mobile phone tracking is now available where parents can sign up to a tracking service through the Internet. They want to sign your phone up to this service, so they can look through the Internet and see where you are at any time.

    1. How do you feel about being monitored through the Internet?

5. The government is leading a stay safe online campaign that focuses on the problems of young people accessing pornography or being stalked.

    1. Have you seen any of these campaigns.

        1. If you have, what are your thoughts on them?

12.5 Questions for Semi-structured interviews – Survivors

Questions to be used for Structured Interview.

Please could you give me an outline of any privacy problems faced by clients caused by modern technology in the following list:
Mobile phones.
Global Positioning Systems (GPS) – eg satellite navigation.
PDAs (small personal hand held computers).
Radio Frequency Tags (RFID).
Internet.
Email.
Information held on databases in external companies, like Utility companies, Phone companies, housing.
Instant Messaging.
Prize Draws.
Loyalty Cards.
Credit Cards.
Cordless Phones.
Public records accessible over the Internet.
Digital Cameras

Have any of the above been used to put any clients at risk?

What advice do you give to people on safeguarding their privacy?

How much of a personal privacy threat do you perceive the following to be, in terms of High, Medium or Low?
Mobile phones.
Global Positioning Systems (GPS) – eg satellite navigation.
PDAs (small personal hand held computers).
Radio Frequency Tags (RFID).
Internet.
Email.
Information held on databases in external companies, like Utility companies, Phone companies, housing.
Instant Messaging.
Prize Draws.
Loyalty Cards.
Credit Cards.
Cordless Phones.
Public records accessible over the Internet.
Digital Cameras

13 Appendix B – Publications

The following publications illustrate dissemination of work within this thesis. The publication by Wood et al is a collaborative work representing an equal contribution of both Wood and Atkinson to the paper. The other authors have contributed guidance. Three selected publications follow.

Atkinson S., Johnson., C., Phippen, AD, (2007), Improving protection mechanisms by understanding online risk, Information Management and Computer Security, 2007, vol. 15, vol. 5

Wood, R, Atkinson, S., Johnson., C., Phippen, AD, (2007), Mobile phones and schools; the development of a taxonomy of risk, In Proceedings of World Conference on E-Learning in Corporate, Government, Healthcare and Higher Education, Canada, October 2007

Atkinson, S., (2007), Technology and the risk to personal safety. Safe: The Domestic Abuse Quarterly, Issue 22, Summer 2007.

Atkinson, S., Johnson., C., Phippen, AD, (2007), Limiting Risks To Personal Privacy Using the Semantic Web, In Proceedings of the Third Collaborative Research Symposium on Security, E-Learning, Internet and Networking.

Atkinson, S., Johnson., C., Phippen, AD, (2007), Personal Privacy Threats: A Taxonomy for Risk assessment. In Proceedings of Second International Conference on Internet Technologies and Applications, September 2007.

Atkinson, S., Johnson., C., Phippen, AD, (2007), Vulnerable Groups and the Impact of Technology Upon Personal Privacy, In Proceedings of Human Aspects of Information Security and Assurance, July 2007

Atkinson, S., Johnson., C., Phippen, AD, (2007),Protecting Society using the Semantic Web, invited poster presentation to the House of Commons Reception for Early Stage Researchers. www.setforEurope.org

Atkinson, S., Jagodzinski, P,.Johnson., C., Phippen, AD, (2006), Semantic Web: A Personal Privacy Perspective, In Proceedings of the Internet Society II: Advances in Education, Commerce and Governance Conference (Ed) Morgan K., brebbia, C.A and Spector j.M, WIT Press, Southampton 2006

Atkinson, S., Jagodzinski, P,.Johnson., C., Phippen, AD, (2006), Personal Privacy: Exploitation or Control through Technology. Proceedings of the sixth International Network Conference, Plymouth, 2006

Atkinson, S., (2006) Internet Technology: How Safe is it? Safe: The Domestic Abuse Quarterly, Issue 16, Winter 2006

Technology and the risk to personal safety: Can Risk to Personal Privacy Be Limited Using Technology?

Background

In the Winter edition of Safe 2005 I wrote about the way that technology was influencing personal privacy and considered how this exacerbated vulnerability. Since then I have been privileged to have interaction with members of Women's Aid who have shared their experiences with me in respect to how the Internet is affecting their personal privacy.

The focus for my research has been primarily on the individual, and how Internet technologies found in modern society now affect the flow of personal information. Whilst there are laws in place that provide a small amount of legal protection, this does not stop unwanted intrusions into our personal lives by commercial enterprises attempting to collect large amounts of data about our preferences and habits. Public data collected by the government is increasingly available online; we see planning permission details, land registry data and civil registrations all available for small fees through the Internet. An increasing amount of information is being collected by the Government. For example, the Information sharing Index will have all children entered on the index by 2008, allowing all children to be tracked (http://www.arch-ed.org/issues/databases/IS%20Index.htm).

Technology is changing the way people communicate. The Internet is becoming an increasingly social space with many people choosing to interact with their peer group through social networking sites such as My Space and Bebo. Mobile phones are getting in on the act too with increasing numbers of phones able to interact in more depth with the Internet. No longer are you limited to receiving emails on your mobile, but now you can enjoy music and video downloads as well as browsing ability. Social interaction can be increased not just with texts and phone calls but uploading to online diaries from the mobile too.

Surveillance technology is also on the rise. A recent report to the Government Information Commissioner by the Surveillance Studies Network (http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf) illustrates the growth in CCTV cameras - the BBC article "Britain is Surveillance Society" [2006] quotes it as being one camera for every 14 people. Increasingly, surveillance tools are entering the reach of the everyday person. CCTV cameras that interact with the home PC are now available for under a hundred pounds. Software called ICAMCU can be downloaded onto a mobile phone that turns the phone into a surveillance device. As mentioned in the previous article, location tracking can be used to determine where a mobile phone is located. For example, Teddyphone, www.teddyfone.com, involves tracking of a mobile phone which is designed to appeal to children under the age of 10.

Research

The objective of the research was to explore the potential for harm brought about by the intersection between Internet connectivity and personal data.
The opinions from members of statutory and voluntary sector bodies in the field of

domestic abuse were sought through interviews and workshops during 2006. Semi-structured interviews were held with two managers of refuges, two outreach workers, and representatives from both Probation and the Police. Two conference workshops with 25 participants were held at the Women's Aid National Conference. Focus groups were carried out where 130 young people discussed personal privacy and their interaction with the Internet. These were backed up through an on-line survey.

Concerns were voiced about the risk potential that the Internet and related technologies posed with regard to the flow of personal information. Primarily concerns were focused on the ease with which personal information was divulged through such mediums such as mobile phones, emails, social networking websites, public records and third party datatabases. Tracking of women to refuges was a major concern. The exact methods utilised by the perpetrators was unknown, but in the opinions voiced by the participants, technology played an important role.

Mobile phones play an important role in the lives of women in the refuges. They provide a lifeline to peers and supporters, yet at the same time allow information about their whereabouts to be ascertained. During my research two refuges discouraged women from using the mobile phones they brought with them, and worked with the network providers to change Sim cards or phone numbers. A number of outreach workers formulated careful plans for communication with their clients and identified a high risk in using a mobile phones, as perpetrators had a tendency for checking the calls made and received, viewing text messages and listening to voicemail.

Sharing information between agencies working with affected families has raised concern. The report by Saunders and Barron (2003) highlights the need for safeguards to ensure that details of a family are not used by perpetrators to track them down. The danger was illustrated when a standard report from a database was electronically transmitted to the perpetrator giving full details of the family concerned. 46% of respondents knew cases where contact procedures had been used to track down a partner [Saunders and Barron, 2003]. This issue highlighted here is that problems are caused by the way in which people are utilising the technology in an attempt to streamline their workload.

Public records were a well known problem. One respondent reported that survivors were advised not to enrol on the electoral register, even though the electoral roll allowed individuals to opt out of having their address publicised. The reasoning being that address information could still be obtained by visiting the local government offices. This tied in well with the findings from the stalkingsurvey.com who found that 17% of stalkers utilised information from public records for tracking, and Sheridan [2005] noted the combination of surveillance, tracking equipment and the Internet.

Tracking refuges through their postcodes was acknowledged to be made easier with the advent of Google Earth, multimap.co.uk, aerial photographs, upmystreet.com and 192.com. Some people made use of Royal Mail PO Boxes to hide real addresses and were not aware that the Royal Mail allocates postcodes for PO Box addresses according to the address of the property, not the nearest post office. Some participants recommended asking the police to get in touch with post offices to let them know that

refuge addresses should not be divulged under any circumstances. In another case one respondent utilised an office address not located near the refuge.

The websites mentioned above show exactly where in the country the postcodes are located. However, it has to be acknowledged that in some cases the resolution of the images is not that clear. One example is that on Google Earth, the postcode for the University of Plymouth, PL4 8AA shows very clearly the buildings on the campus as does the aerial photograph from multimap.co.uk. However, in comparison the YHA River Dart, postcode TQ5 0ET is not visible.

192.com and multimap.co.uk were mentioned by name in the research. One refuge contacted BT (192.com) to ask for the map pointer to illustrate an alternative location when the refuge postcode was entered. This request was granted.

Increasingly, access to computers for residents is becoming important, especially when there are children involved. Homework and coursework has become reliant upon Internet access. Many housing authorities require bidding to be carried out online and increasing numbers of local authority and social services interactions are being moved online. However, this approach provides headaches for the refuge managers. Residents are now being tempted to give out personal information, names, addresses, and locations. They are also tempted to divulge information about individuals within the refuge or organisation.

The main issues to emerge from these findings were that there was a requirement to:

- Identify where risks lay
    - For example with tracking devices and the way they interact with the Internet.
- Identify where individuals or refuges are located through the use of postcode identification and mapping software
- Identify and control personal information given out by residents
    - About themselves
    - Or about other people.

Prototype

It became clear that giving out personal information was a risk and as such needed to be controlled. The next stage in the research was to design a device to help individuals online. Based upon the findings of the research, a prototype Internet Explorer browser plug has been designed with the objective to inform the users about the consequences of their actions and to highlight where their personal information was being divulged.

The software works in the background of Internet Explorer 7 and gives a simple warning if a website is collecting information. Different elements of information are given different weightings and a simple traffic light system of warning colours used, with the postcode having the highest warning rating of red. A breakdown is given of where personal

information has been divulged, keeping a record of what information has been divulged to which URL. Users of the software can return to the URL to explore further issues connected with privacy policies or to request that their information be removed.

In addition, the software uses the search engines to discover information already held on the Internet about the user. Searches are made using combinations of name, address, postcode and work place. These URLs are presented to the user so that they can determine what the effects would be when combined with information they give out.

Evaluation

The next phase is for the prototype software to be evaluated. This is to determine whether taking a more informative rather than restrictive approach would affect individual behaviour. The aim is to reduce the amount of information being given out, the argument being that if this is reduced, the risk of harm to an individual will also be reduced. Early evaluation has proved very positive, with one teenager remarking:

> "Yeah, this would make me think a bit more about what I put out and where! It's nice to know what I've said".

With this in mind I would like invite participants to contact me at the address below:

Shirley Atkinson
Network Research Group
School of Computing, Communications and Electronics
Room A304
University of Plymouth
Portland Square
Plymouth
PL4 8AA

shirley.atkinson@plymouth.ac.uk
www.network-research-group.org

References

BBC, (2006), Britain is 'Surveillance society', http://news.bbc.co.uk/1/hi/uk/6108496.stm, Thursday 2 November 2006

Saunders, H., Barron, J., (2003), Failure to Protect?. Women's Aid, Bristol.

Sheridan, L., (2005)., Key Findings from www.stalkingsurvey.com., University of Lancaster, date accessed 25/05/06

PERSONAL PRIVACY THREATS: A TAXONOMY FOR RISK ASSESSMENT

Shirley Atkinson[1], Christopher Johnson[2] and Andrew Phippen[1]

[1]Network Research Group, University of Plymouth, UK
shirley.atkinson@plymouth.ac.uk
[2]University of Plymouth, UK
c.johnson@plymouth.ac.uk

ABSTRACT

The explosion in the use of the Internet and the growth of the volume of available data has made collecting personal information about an individual easier than ever before. Problems faced by vulnerable individuals which stem from the abuse of gathered information are exacerbated. Abuse and harm of individuals, through grooming, harassment and bullying, coexist with identity theft as examples of criminal behaviour that are, aggravated by the ready availability of personal information. This paper presents a Taxonomy of threat to be utilised when assessing risks to vulnerable individuals and concludes with a description of the application of our taxonomy to five social networking websites.

KEYWORDS

Internet, Personal Privacy, Teenagers, Domestic Abuse Survivors, Semantic Web

1. INTRODUCTION

Modern privacy problems have been identified as a result of unchecked information flows between a variety of different entities [1]. The ubiquitous nature of the Internet facilitates the gathering, storage and onward transmission of personal data - something which business enterprises turn into a commodity [2]. One impediment to the free flow of information between entities has been the format of data, in that not all formats have been recognised or accepted. The Semantic Web [3] concept aims to address this issue and provide the standards required to allow data to be shared in a more seamless fashion.

Personal information is a difficult entity to control, once it has been divulged it is difficult to ascertain exactly where else it may be divulged. As Tavani [4] highlights the three types of threat to personal privacy add to the complexity of protecting personal data: implicit or explicit data gathering techniques; data exchange techniques; and data mining techniques add to the pressure upon personal data. Social networking web applications, where individuals link to each other give a good example of uncontrolled data exchange. One thing divulged to a friend with a direct link can then be observed by somebody else who does not have a direct link.

Divulging information is observed in two distinct areas: the personal information explicitly given through personal websites, on-line diaries and other internet-mediated communications that encourage individuals to divulge their information; and public personal information [4], the information about an individual held by third parties such as the government. Public records have always been available to those who take the time to enter public buildings and examine them, however, government services now provide access to public records through the Internet.

Examples of these are planning application details, and access to the general record office indexes of births, marriage and deaths.

Divulging personal information does not in itself pose a problem, however problems arise when the information divulged is abused. In this respect some individuals are considered more prone to harm than others. Abuse and harm of individuals, through grooming, harassment and bullying, coexist with identity theft as examples of criminal behaviours, all aggravated by the ready availability of personal information. Posting information on social networking websites has been linked to murder [5]; Bocij [6] identifies the Internet as a tool for stalking behaviour; Southworth et al [7] illustrates how modern technology is being used in situations of domestic abuse; and Mitchell et al [8] and Hughes [9] observe how the Internet has facilitated sexual exploitation of women and children.

In this paper we present a taxonomy of threat designed for use within risk assessment. This taxonomy has been designed by examining the problems faced by vulnerable groups with regard to the impact of the Internet upon their personal privacy. In section two we introduced the methodology, describe how the vulnerable groups were selected and the research methods used. In section three the findings are presented and section four presents the taxonomy and applies it to a selection of social networking websites. Section five concludes with the direction for future research.

2. METHODOLOGY

Raab and Bennett [10] propose that more effective privacy solutions are created by focussing on the privacy issues for vulnerable groups. With this in mind, two groups were selected, a discussion of this selection is given below in section 2.1. Qualitative research methods were utilised to explore the social context [11] within which those groups found themselves, these methods are described in more detail in section 2.2. The data collected was considered to be responsive to their thoughts, feelings, experiences and behaviours [12] which would allow a richer understanding of their personal privacy situation. Taking note of the complex interplay of issues would therefore lead to an enhanced understanding of the social context, which in turn would lead to more meaningful action to be taken. For the mitigation of risks to be effective, a good understanding of the factors involved is required and the qualitative approach lends itself to gaining that understanding.

2.1. Selection of Vulnerable groups

Two groups were considered to represent vulnerable groups for the purposes of this research, domestic abuse survivors and teenagers.

Domestic abuse survivors, hereafter referred to as Survivors, exhibit vulnerability in different situations. As a group of individuals they are most likely to experience "dataveillance" [13] technologies being used against them. Whilst Survivors will face many violent and controlling episodes before they seek help [14], the time when they are at their most vulnerable is when the decision to leave the abusive relationship and seek refuge is made [15]. Any release of personal information at this time can lead to serious harm or death.

Teenagers have been identified by Magid [16] as those most at risk from predatory behaviour. These young people increasingly explore the boundaries of the technology that surrounds them, often in such ways that their parents do not understand and therefore find difficult to monitor. The Internet has become more of a social space with many of them creating and uploading content [17] through the many and varied social networking websites. These teens utilise the different web

applications as a way of keeping up with their peers and often do not consider the consequences of their actions. Advice given by the government education campaigns [18], and by researchers [7; 19] centre around keeping personal information private. However, here lies the dichotomy: young people should keep their information safe, but they want to share it with their friends using the technology that is part of their social world.

2.2 Research Methods

The opinions from members of statutory and voluntary sector bodies in the field of domestic abuse were sought through interviews and workshops. Focus groups were carried out where young people could discuss their views on personal privacy and interaction with the Internet. These were backed up through an on-line survey.

Semi-structured interviews were held with two managers of refuges and two outreach workers; two conference workshops were held at the Women's Aid National Conference. The participants of the workshops were workers from both refuges and outreach services, all working with domestic abuse survivors. The workshops were aimed at exploring the uses and abuses of technology.

Seven focus groups were conducted involving teenagers; two were held with year twelve teenagers, one with year ten and another with year eight. Four more focus group transcripts were made available from the Trustguide[3] project which utilised a similar methodology and questions. Prior to conducting the discussions the young people within the focus groups were issued with a questionnaire designed to elicit some broad demographic data around their Internet usage. The discussions were generated by describing a set of scenarios based upon an understanding of the problem situation, and encouraging the respondents to discuss their views, thoughts and feelings that the scenarios generated. The discussions were recorded onto tape for later transcription which were analysed using N6 software to extract the concepts. The concepts emerging from the data were refined and structured into the taxonomy that is presented in the next section.

3. FINDINGS

Those who had responsibility for the safety and well being of others, managers of refuges, and teachers, voiced their concerns about the risk potential that the Internet and related technologies posed. Primarily their concerns were connected with the ease with which personal information was divulged through such things as mobile phones, emails, social networking websites, public records and third party databases.

Examples were given where personal information made available through the Internet had compromised women's safety; 83% of the teenagers interviewed divulged personal information with 27% expressing concern about having done so.

Teenagers employed a variety of coping mechanisms: they made good use of any blocking techniques made available by the different software used; where requests for personal information were considered to be excessive, these were ignored or if the request was mandatory, false information supplied. However, the descriptions given by the teenagers of the information they divulged did not entirely match the public information given by themselves in social networks. For example, some chose to claim they were older than they really were, others posted photographs of themselves wearing revealing clothing. On examining the top three social networking websites listed by the teenagers, each of the schools taking part in the focus groups had a substantial presence on them.

[3] http://trustguide.org.uk

4. TAXONOMY OF THREAT

Focussing upon the concerns raised by teachers and managers of refuges, the data collected was evaluated to ascertain where personal privacy risks to teenagers and survivors lay. Risk categories were identified in terms of the potential impact where damage to personal privacy could take place; where threats to giving out personal information might lie; and where there was a potential for unwanted intervention.

Within these three areas, the manner in which the risks to individuals manifested themselves were considered within four different categories:

e-Sociability
: This considered the act of being sociable within the electronically connected context and examined the methods employed for keeping in touch with peers.

Data boundaries
: How individuals determined what elements of personal data needed protecting and how boundaries were set around personal data.

Access control
: Once the boundaries were determined, consideration was given to how they were enforced, along with who provided the tools to enforce those boundaries.

Technological impact
: Consideration was given to the effects the technology had on an individual's behaviour.

Our taxonomy of threat has the form illustrated below in table 1.

Table 21: Taxonomy of Threat

	Propensity for Harm	***Divulging Personal Information***	***Unauthorised Intrusion***
e-Sociability	Manifestation of risk		
Data Boundaries			
Access Control			
Technological Impact			

Risk assessments are usually carried out by experts within a field to consider specific hazards and give proposals on how to minimise or remove the identified risks. However, problems arise in a number of ways. Internet devices, their uses and impacts pose many different hazards in many different situations. Problems also arise when different experts attribute different meanings and weightings to risks. Utilising a framework provides consistency and by basing the framework upon a taxonomy a less restrictive approach structure will allow risks to be evaluated. Different experts can utilise the same taxonomy structure but have the ability to adapt the structure to different local contexts [20].

A taxonomy is an organised structure that serves as a useful lens for classifying and understanding a body of knowledge [21]. Concepts are logically ordered into groups and categories as illustrated in Table 1 thus allowing preventative measures to be applied.

4.1 Existing Taxonomies

There are three taxonomies proposed that are connected with personal privacy: the Privacy Goals Taxonomy [22], Young people and risk on-line [23] and the Taxonomy of Privacy [24]. The first from Anton et al [22] primarily focuses upon business privacy data and the field of commerce. Existing threats to consumer privacy are categorised into seven classes of threat. The second taxonomy developed by the Cyberspace Research Unit at Lancaster is more relevant than the first to the problems faced by teenagers [23]; behaviours are represented in terms of physical, psychological and social well being of children and young people. The third taxonomy proposed by Solove [24] identifies different privacy harms and problems that have already achieved a significant amount of social recognition. Four categories and many related sub-categories are identified: Information Collection, Information processing; Information dissemination and Intrusion.

Whilst these existing taxonomies assist in providing different viewpoints of the privacy field, they concentrate on different areas to that which has been examined in our research. The Taxonomy of Threat introduced in Table 1 is discussed further by use of an example below.

4.2 Social Networks

To demonstrate how the taxonomy presented in table 1 assists risk assessment, it is applied to an assessment of a selection of five social networking web applications: www.myspace.com, www.bebo.com, www.spaceslive.com (Windows Live Space), www.facebook.com and www.zorpia.com. These applications were sampled from those listed by teenagers in the questionnaires.

4.2.1 E-Sociability

The Internet provides different methods for young people to keep connected with their peers either through Internet-mediated communication such as emails and messenger, but also through web applications and social websites. "Blogging", creating on-line diaries, has become a popular past-time and is considered to be a growing phenomenon [25] but one which has been identified by CEOP [26] as an area of concern. McMillan and Morrison [27] observe how young people build their community around the interactive technologies.

New Nokia phones contain LifeBlog software offering the ability to create an on-line diary, a blog, whilst on the move. O2 encourages people to upload content in return for payment [29] and video social networking websites such as YouTube are launching the facility to use mobile phones to view the videos posted on the website [30].

Gross et al [31] suggest that the interface of social networks combined with peer pressure, herding behaviour, and short-sighted privacy attitudes contribute to the situation where young people reveal quantities of personal information.

Each of the applications considered allowed people to link and connect with each other. Common features include photographs and some form of comment whether in the form of blogs, journals or discussion boards. MySpace, Bebo and Facebook all link people together in groups; these can be based on school, university or the workplace. Bebo and Facebook provide differing levels of control over who joins the different groups. In the case of Bebo you cannot join a group uninvited, another member must enrol you. Facebook allows you access to school networks for two weeks before removing you from the group if you have not been accepted by another member of the group. Bebo, Facebook and MySpace offer a multimedia rich environment allowing music and videos to be shared and played. Zorpia is aiming at the over 16 year old market. Facebook provides the facility to upload photographs and place description tags of individual's within the photographs that link to the personal profiles of those people.

A summary of the potential risks is given below:

Table 22: e-Sociability Summary

Propensity for Harm	*Divulging Personal Information*	*Unauthorised Intrusion*
Personal data gleaned for use in situations of bullying, stalking and harassment.	Photographs, blogs, journals, discussions linked to personal profiles. Name and address used in search and display terms.	Photographs and video's uploaded by third parties. Access to profiles through friends rather than direct link.

4.2.2 Data Boundaries

Tavani [4] identifies personal data in two areas: public personal data and normative personal data. Normative personal data is where an individual would expect their data to be kept private. The public personal data has boundaries placed around it that are not under the control of the individual to whom the data belongs. Third party actions upon these boundaries can cause issues of concern. One area of concern is the release of public records, for example the electoral role, combined with the information released through social networks. This data boundary is infringed when websites contain personal data that has been posted by other individuals.

Each of the five websites collect and display a wide variety of personal information. As a minimum MySpace collects first name, last name, postcode, country and email address. The others following similar lines. Each allow personal photographs to be uploaded. Facebook and Zorpia do not make as much information mandatory.

Table 23: Data Boundaries Summary

Propensity for Harm	*Divulging Personal Information*	*Unauthorised Intrusion*
Linking postcode to mapping applications. Linking date of birth to GRO indexes to obtain mothers maiden name.	Profile made public. Third parties divulging information.	Third parties posting photographs, names, addresses and other personal details.

4.2.3 Access Control

The approaches and tools for profile protection differ between the five websites. Facebook is the only website to offer a fine-grained approach to controlling what is made publicly available. Many of the personal data elements can be toggled between public or friends only viewing. Photographs that are tagged with an individual's name are notified to that individual, thus allowing them the opportunity to request their removal if required. Profiles and photographs of individual's can only be seen once a link has been made and approved by the other party.

Bebo allows the whole profile to be made private only. Each of the websites assessed allow the individual to hide their date of birth, friends who have made connections are easily seen along with their friends. They allow you to browse freely the friends of friends who are connected to your

profile.

Searching for individual's differs amongst the websites, some allow searching for individual's by location, age and gender, others are more restrictive only allowing searching to be carried out on networks that the searcher has been invited into. Zorpia allows searching to be carried out by gender, age and location. MySpace uses first name, last name and location for the searching and state in their privacy policy that pictures and first names will be displayed to users who search for you. Windows Live Space and Bebo provide a free text search box and do not have a facility to refine the search any further.

Table 24: Access Control Summary

Propensity for Harm	*Divulging Personal Information*	*Unauthorised Intrusion*
Search on location, gender, age.	Control of profile vs finer grained control of individual data elements. First name and photograph returned in search.	Tagging and linking of photographs. Searching

4.2.4 Technological Impact

Each of the websites allows and encourages personal information to be shared, however each has a different approach to protecting the user's privacy.

MySpace is the only one to make the majority of important personal information mandatory to join the site. First name, last name, email address, postcode, country and gender are all essential for registration, date of birth however can be omitted. It does provide safety tips and the privacy policy from links at the bottom of the page and the registration page reminds potential users that their data will be stored and bound by US data rules.

Bebo and Windows Live Space make more of the interaction with CEOP and blog safety campaigns by placing the links to report abuse and safety guidelines in prominent positions. Bebo places reminders for those under 21 next to the text boxes so that the safety tips are more prominent. Zorpia, being aimed at those over 16, carries no such warnings.

Table 25: Technological Impact

Propensity for Harm	*Divulging Personal Information*	*Unauthorised Intrusion*
Lack of safety warnings on some sites	Important personal information mandatory for registration	Data control rules applied from different country.

5. CONCLUSIONS

By applying the taxonomy of threat as detailed in Table 1 to the field of social networking applications, issues that pose potential for risks to individuals can be highlighted and from there action can be taken by individuals or those who have responsibility for other individuals.

The results from the early stages of the research indicate that individuals use of Internet technology should be combined with empowered, informed consent. Technology should therefore be designed to facilitate an individuals control of the flow of personal information.

The next phase of the research is to evaluate the success or otherwise of a technological approach in providing privacy protection whilst using the Internet. Evaluation of the technological approach is to be carried out by the user groups themselves. The effectiveness will be assessed in terms of the understanding and perception of levels of control of personal information and understanding the potential consequences for actions taken.

REFERENCES

[1] Solove, D.J, (2004), *The Digital Person*, New York University Press, New York

[2] Tynan, D, (2005), *Computer Privacy Annoyances*, O'Reilly, USA

[3] Berners-Lee T, (2000), *Weaving the Web*, Texere, London

[4] Tavani, H.T, (2007), *Ethics and Technology 2nd Edition*, Wiley, USA

[5] Wired News, (2006), *Teens Reveal Too Much Online*, Associated Press, 5th February, 2006, http://www.wired.com/news/wireservice/1,70163-0.html, date accessed 31/01/07

[6] Bocij, P, (2004), *Cyberstalking*, Praeger, Conneticut

[7] Southworth, C., Dawson, S., Fraser, C., Tucker, S., (2005), "A High Tech Twist on Abuse: Technology, Intimate Partner Stalking and Advocacy", *Violence Against Women Online Resources*, Minesota, www.mincava.umn.edu/documents/commissioned/stalkingandtech/stalkingandtech.html date accessed 31/01/07

[8] Mitchell KJ, Finkelhor D, Wolak J, (2005), "The Internet and family and acquaintance sexual abuse", *Child Maltreatment*, Vol. 10, No. 1, pp49-60.

[9] Hughes, D.M., (2003), "Prostitution online", *Journal of Trauma Practice*, Vol 2. No 3/4, pp115-132, www.uri.edu/artsci/wms/hughes/internet.pdf, date accessed 31/01/07

[10] Raab, C.D and Bennett, C.J, (1998), "Distribution of Privacy Risks: Who Needs Protection", *Information Society*, Vol 14, Issue 4, p 263-274

[11] Dahlberg, L., (2004), "Internet Research Tracings: Towards Non-Reductionist Methodology", *JCMC*, 9 (3) April 2004.

[12] Strauss, A., Corbin, J., (1998), *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, Sage, London

[13] Clarke, R, (1999), *Introduction to Dataveillance and Information Privacy*, Xmamx Consultancy Pty Ltd, www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#Intro date accessed 31/01/07

[14] Yearnshire, S. (1997) "Analysis of Cohort" in: Bewley, S., Friend, J. and Mezey, G. (Eds). *Violence Against Women* London: RCOG

[15] Womens Aid Federation of England, (2002), Domestic Violence Statistical Factsheet 2002, http://www.womensaid.org.uk/dv/dvfactsh2002.htm date accessed 31/01/07

[16] Magid, L, (2004), *Teen Safety on the Information Highway*, National Center for Missing and Exploited Children, www.safeteens.com/safeteens.htm#Guidelines_for_Parents_0, date accessed 31/01/07

[17] Lenhart, A., Madden, M, (2005), *Teen Content Creators and Consumers*, Pew Internet & American Life Project, Washington www.pewinternet.org/pdfs/PIP_Teens_Content_Creation.pdf, date accessed 31/01/07

[18] Fiveash, K, (2006), *Internet safety talks for UK kids*, The Register,

www.theregister.co.uk/2006/09/20/internet_children_safety/ date accessed 31/01/07

[19] CRU, (2006), *Internet Safety Zone*, Cyberspace Research Unit, University of Lancaster, www.internetsafetyzone.co.uk/root/default.htm date accessed 31/01/07

[20] Kemshall, K., McIvor, G, (Eds) (2004), "Managing Sex Offender Risk", *Research Highlights in Social Work 46*, Aberdeen

[21] Carr, M.J., Konda, S.L., Monarch, I., Ulrich, F.C., Walker, C.F., (1993), *Taxonomy-based Risk Identification*, sei.cmu.edu, www2.cs.uh.edu/~zhibinma/tx.pdf, date accessed 31/01/07

[22] Anton, A.I., Earp, J.B., Reese, A., (2002), "Analysing Web Site Privacy Requirements Using a Privacy Goal Taxonomy", I*n Proceedings of 10th Anniversary IEEE Joint Requirements Engineering Conference (RE'02)*, February 2, 2002

[23] O'Connell, R., Bryce, J., (2006), *Young People, Well Being and Risk Online*, Council Of Europe, http://www.coe.int/t/e/human_rights/media/1_Intergovernmental_Co-operation/MC-S-IS/H-inf(2006)005_en.pdf date accessed 31/01/07

[24] Solove, D, (2006), "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, Vol 154, No 3, p477

[25] BBC, (2006a), *Blogging set to peak next year*, BBC, 14 December 2006 http://news.bbc.co.uk/1/hi/technology/6178611.stm, date accessed 31/01/07

[26] CEOP, (2006), *Blogs, Think You Know*, www.thinkuknow.co.uk/control/blogs.aspx, date accessed 31/01/07

[27] McMillan, S.J. and Morrison, M, (2006), "Coming of age with the Internet", *In New Media & Society*, Vol 8 (1), PP 73-95, Sage, London

[28] Briscoe, K, (2006), "The schoolchildren bullied by email and text", *Evening News*, 17 November 2006

[29] O2, (2006), *LookAtMe*, O2, www.o2.co.uk/fungames/lookatme date accessed 31/01/07

[30] BBC, (2006), *YouTube moves to the small screen*, BBC, 28 November 2006 news.bbc.co.uk/1/hi/technology/6190984.stm date accessed 31/01/07

[31] Gross, R., Acquisti, A, (2005), "Information Revelation and Privacy in Online Social", *Proceedings of the 2005 ACM: Workshop on Privacy in the Electronic Society*, pp71 - 80

Vulnerable Groups and the Impact of Technology upon Personal Privacy

S.Atkinson[1], C.Johnson[2], and A.Phippen[1]

1. Network Research Group, University of Plymouth, Plymouth, United Kingdom
2. University of Plymouth, Plymouth, United Kingdom
email: shirley.atkinson@plymouth.ac.uk

Abstract

Privacy for the individual has become more of a concern as use of the Internet increases. Social websites that facilitate sharing of photographs and personal information potentially increase the risk of harm through harassment and bullying thus leading to serious physical or mental harm. Vulnerability is perceived in new technological development and privacy enhancing technologies (PETs) do not fully address the vulnerability issue. This research presents a view of privacy issues for two vulnerable groups, teenagers and domestic abuse survivors and concludes with how technology might address some of the vulnerability issues.

Keywords

Privacy, Vulnerability, Domestic Abuse, Teenagers, Technology

1 Introduction

The intersection between personal data with Internet connectivity and the resultant potential for harm is an area of increasing concern. The media make much of the potential threats to privacy (BBC News, 2006, Ward, 2006a, Ward, 2006b) highlighting the latest technology and the potential for harm. Privacy activists utilise the Internet to promote their campaigns for confidentiality and protection of personal data (Caspian 2004, The Big Opt Out 2006, No2ID 2007, Spychips 2007). Furnell (2005) highlights the issues faced by Internet users, suggesting that the primary threat motivations are usually "mischief or money".

However a more serious potential for harm is seen with harassment and bullying coexisting with identity theft. These examples of criminal behaviours are exacerbated by the ready availability of personal information. Social networking websites have been linked to murder (Wired News, 2006); Bocij (2004) identifies the Internet as a tool for stalking behaviour; Southworth et al (2005) illustrate how domestic abuse is made easier with modern technology; and Mitchell et al (2005) and Hughes (2003) observe how the Internet has facilitated sexual exploitation of women and children.

The combination of this serious potential for harm with the evolution of the Internet into a more social space and the convergence of mobile phones with the Internet, leads to some disturbing issues. Websites share photographs, information, arrangements to meet friends and online diaries or 'blogs'. Both the European Commission (EU) and the UK Home Office have taken action to address the issues for harm: the EU Safer Internet Programme (2006) unites European countries aiming to provide a safer online environment for children; the Home Office initiated the Child Exploitation and Online Protection Centre (2006). Government education campaigns (Fiveash, 2006), and researchers (Bocij, 2006; CRU, 2006) give advice that centres around keeping personal

information private. However, here lies the dichotomy, young people should keep their information safe, but they want to share it with their friends using the technology that is part of their social world.

This paper presents an outline of technological approaches to privacy and their limitations before presenting the study into the issues faced by individuals for whom privacy is of serious concern. The findings from the study are presented followed by a discussion on how technology might be utilised to address some vulnerability issues.

2 Technological Solutions

Privacy enhancing technologies (PETs) and privacy aware technologies (PATs) attempt to address some of the concerns surrounding the control of personal information: PETs minimise or eliminate the collection of identifiable data (HISPEC, 2002); PATs are designed, developed and deployed with privacy in mind (Cannon, 2004). Limiting factors are seen in the deployment and usage of PETs: weak tools within distributed systems (Goldberg, 2003); explicit choice between anonymity and identity (Burkett, 1997); and lack of awareness of threats by the individual (Furnell, 2005). Those in favour of PATs suggest better protection is afforded when privacy measures are incorporated into design (Givens, 2000), or when technological and social approaches are combined to provide the best privacy toolkits (Goldberg 2003, Raab 2004).

Garfinkel (2000) suggests that developers create naturally privacy invasive solutions by ignoring the need to protect personal information, leading to lack of control for the individual. Solove (2004) also describes technology as creating an "architecture of vulnerability" where individuals are placed at risk, yet powerless to take any action, giving identity theft as an example of this. The Fraud Advisory Panel (2005) identify technology as providing new approaches for fraudulent behaviour, changing the boundaries of how criminal behaviour takes place. Disclosure (Dinev and Hart, 2004) and lack of control of personal information (Margulis, 1977) has been directly linked to issues of vulnerability.

One issue to emerge from criticisms of the technological approach is how best to inform design. To this end, Raab and Bennett (1998) propose that studying privacy issues for vulnerable groups would enhance the technological design for personal privacy protection.

3 Study of Potential for Harm

Two groups of individuals were chosen as those who most exhibit issues of vulnerability: Domestic abuse survivors (hereafter referred to as Survivors) and Teenagers. For these groups the lack of control of personal information has some serious consequences: Survivors are at most risk when they decide the leave an abusive relationship (Women's Aid, 2002); Teenagers make full use of the Internet as a social networking tool and are considered most at risk from predatory behaviour (Magid, 2004).

Methodology

Qualitative approaches to collecting information were adopted as the most appropriate way to study the social context (Dahlbert, 2004) and to gain an understanding of how the different complexities

involved were experienced (Feenberg, 1999). Semi-structured interviews were held with: refuge managers; providers of Survivor's outreach services; and probation and police officers. Front line staff were selected as those best able to give an overview of the situation without being under emotional duress. Focus groups were held involving 105 teenagers from the South West of England, with an average age of 14.7 years and a fairly even gender balance. An online questionnaire distributed through snowball sampling collected opinion about different privacy scenarios concerning the Internet.

4 Findings

Whilst the issues for Survivors and Teenagers fell into different categories, there were some similarities. Tracking of Survivors was felt to be the primary concern, whether technologically assisted or through methods best described as "social engineering" (Mitnick and Simon, 2003). Teenagers did not see any problems with sharing their personal information on specific websites, but they did view with suspicion websites that wanted to gather personal information for which there was no obvious reason. Some described unwanted contact and how they had dealt the situation.

Survivors

As Abrahams (2007) highlights the safety of Survivors relies heavily upon protecting the security of the refuge, ensuring that even inadvertent actions do not compromise safety. Of primary concern therefore, was how technology provided abusers with the tools and information necessary to carry out abusive or controlling behaviour. Tracking of safe houses or refuges through divulging of address information; continuation of harassment and controlling behaviour through the use of mobile phones; residents use of the Internet in refuges; and data protection controls of third parties were all expressed as concerns.

Tracking

Examples of tracking were given where location information had been gleaned through Internet resources or mobile phones. One woman had been traced through her Internet banking, it was not beyond the realms of possibility that pin numbers and personal questions were known or easily calculated by an intimate partner. In another situation, a perpetrator had access to data held in the Drivers Vehicle Licence Authority (DVLA) database which was provided to his place of work through an Internet connection. The registration number of the support workers car was traced which in turn provided the address. The perpetrator was therefore able to discover which refuge the Survivor had fled to.

One respondent described the elaborate security details that the support services had created, only to be overturned by a member of staff at a utility company divulging the address.

- "She'd had high level security around moving in .....He'd got the address from the gas board because he rang and said that he was aware that they'd turned it off but unfortunately he couldn't remember the house number and they actually gave the full postal address. The lengths that that woman had gone to, ...even the removal men didn't know the address they were taking her to until the van was laden. .....That is awful when somebody has gone to that length to be safe and it's been taken away. For three days they'd had the only peace of mind that they'd ever known, and even then, they were anxious about going out to the shops or anything. Then there he was on the door. He actually said that was how he tracked her down."

Mapping websites such as Google Earth, multimap aerial photographs, upmystreet.com and 192.com caused concern for refuges because of the way that the Royal Mail allocate post box numbers. P O Box postcodes are allocated according to the address of the property, not the nearest post office. The mapping websites show exactly where in the country the postcodes are located and provide aerial images in some cases. One manager of a refuge spoke of her despair at trying to remove their postcode from a mapping website.

> "it just makes a mockery of everything that we try and achieve in terms of confidentiality and secrecy and just to think anybody could log on to that website and have a pretty good idea of where we are, and the fact that we can't get it removed either."

Mobile Phones

Mobile phones were considered problematic in providing constant communication between the Survivor and the perpetrator as well as issues surrounding location tracking. One refuge manager described how mobile phones almost negated the work that the refuge was trying to carry out.

> "In terms of the old days, if women fled they could get away from their partners without their partner knowing where they were ..... Often the fact that women come with mobile phones and partners have access those numbers, means that there's all sort of different issues .....you do occasionally have situations.....where a woman is in the refuge and they talk to their partners.....which just seems a bit of an irony,.....in that they are in a refuge to get away from them in the first place, ...where he has attacked them and the police have come to get them, and they are actually talking to them. "

Women in the refuges were encouraged to change their phone numbers and in most cases were provided with new Sim cards for their mobile phones. Despite this, two respondents described incidents where new mobile numbers had been discovered by the perpetrators. Mobile phones were also common presents to children of the relationship and therefore caused concern over location tracking services being used. One outreach support worker described how survivor's mobile phones would often be checked by perpetrators.

> "Most women who have mobile phones will say that they're partners check their phones, they check them for numbers, they randomly ring the number, they'll answer them"

In addition to these actions, the support worker was certain that a client of hers had been traced using her mobile phone.

> "We've had problems in the past where, and I don't understand the technicality of it, but whereby partners of women who've got mobile phones have been able to actually track where they are from the phone."

Data Control

For those remaining within the home environment, emails and Internet history being monitored were a well known issue. Survivors were described as being more likely to be fooled by spam and phishing emails.

> "When you see things like that it is, especially if you are vulnerable, you can sometimes be easily swayed."

Other forms of harassment were described where personal details had been posted by perpetrators to advertise sexual services.

Within refuges computing facilities were provided to Survivors primarily for two reasons: housing authorities were now using online bidding for housing; and resident's children needed access to assist with their education. However, two new problems were identified:

4. personal information was freely divulged by the residents about themselves and about other residents.
5. Gambling, pornography, online dating websites accessed.

The effectiveness of privacy controls utilised by third parties storing personal data about service users was raised as a concern. The effect of the Freedom of Information Act had been felt when one perpetrator had used the right of access to information to discover the safe-house location of the family. In another situation the support worker had to take great care over how rehousing information was to be held:

> "a woman working for the local authority who wanted to access our service who's partner worked for the city council too, and was very anxious about what we held on computer and what information we sent in. Because we were assisting with rehousing and they were actually anxious about who had access to that information within the city council, whether it was held and maintained in that individual section, or whether it would be accessible because her partner was in a position where she thought he may be able to find out that information. So there has been a number of cases like that I think where people have been anxious. "

Teenagers

The findings from the focus groups were very much in keeping with what was expected: 83% of young people interacted online; 62% gave out personal information as part of a registration process. What was noteworthy was that 27% expressed concern about having given out information. Figure 1 illustrates a fairly even gender split of those who signed up and those who were concerned.

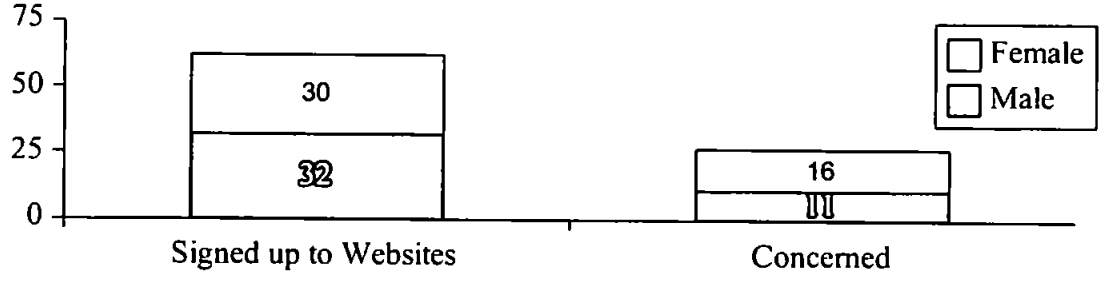


Figure 1: Gender split on disclosing Personal Information

Internet Usage

The majority of young people said they made use of the Internet for: homework; revision; referencing Wikipedia; searching for information for work; school work; and coursework. Social uses were described which included interaction with friends; playing games; and downloading music or videos. Connecting with friends from school was a major activity with only one person admitting to using the Internet to meet new people. Control measures were utilised on occasion where the ability of messaging software to block people was utilised.

52 different websites were listed as having collected personal information from the respondents, with the top three being social networking sites. The most common sites were MSN Space, Bebo, and My Space which have differing privacy approaches. My Space made it easy to find people by school and allowed a search for young people between the ages of 16 and 18, however with Bebo a search could not be made of a young people at a specific school unless invited by somebody who was already a member. At the time of researching the websites, MSN Spaces was upgraded to Windows Live Spaces which appeared to have stronger privacy controls allowing different public and private profiles to be created.

Most young people knew that large amounts of information should not be given out, one respondent passed comment on the apparent naivety of individuals who posted large amounts of personal information on the web, suggesting that these must be younger people who did not have an idea of the potential dangers. This protection of information also related to websites that collected quantities of personal information during the registration process. Many young people evaluated the websites to determine which requests for information were really necessary.

> "..... Or rather, it concerns me how much some websites ask for when I can't see why they would need the information or if a website asks for an email address for what would appear to be to gain nothing particularly. I don't give my information to them. I use my hotmail"

Mandatory fields collecting personal information that were considered to be in excess of what was necessary, were circumvented with false information or aliases frequently used. One respondent described making up a false address in order to circumvent the need for American zip codes. Multiple email addresses were used in some cases, one for signing up to websites, and another for personal use.

Bad Experiences

Most teenagers answered "No" when asked if they had any bad experiences using the Internet with two notable exceptions. One described looking for information about a basketball team, and on clicking the hyperlink being confronted with pornography; another described pornographic material sent to his hotmail account which had to be shut down.

Being contacted by strangers through MSN Instant Messenger was mentioned in five different groups, but was not explicitly considered to be a bad experience. One group of girls described men discovering their email addresses on the Internet, making contact and suggestive remarks; one student could trace the increase in spam emails to when his friend had published his email address on the Internet; another described an interaction through MSN with somebody who at first appeared to be a friend of theirs, but later transpired not to be; another girl described how her suspicions were aroused when conversing with somebody claiming to be 13 years old saying:

> "This guy, like * he added me and I just accepted him thinking oh, I don't know who it is. He said he lived far away. He said where do you live, and I goes **, and he said where's that? and he didn't know. So I thought, everyone knows where ** is and he said I don't . Then I said how old are you and he said he was 13. Then he like showed a picture and he looked loads older, and then started saying like loads of weird things to me, so I thought, then I showed my mum and she said there's no way he's like 13 and stuff like this."

Being contacted by strangers was not the only thing to make some young people feel vulnerable.

Another person described taking part in an online game which included a large number of players speaking French. As he did not speak French he could not understand what they were saying, but noticed his name being mentioned many times, which in turn led to his feeling very insecure.

Three people described financial losses: one had an e-bay purchase that went wrong; another had a credit card fraudulently used through e-bay; and the final one was from a prize draw scam.

> "It said we'd won something, then we clicked on it and then it says you ring up. So we rang up and then it said, give the bank details. We'd done it before and it's just then she got scammed over thousand pounds and lost pounds from her bank account. But then the bank could do nothing about it."

5 Discussion

The findings illustrate the effects on individuals when personal information is released, whether they have explicitly released the information themselves or another party has done so. Previous work by Margulis (1977) and Dinev and Hart (2004) correlated the release of personal information to vulnerability, the more personal information released, the more vulnerable an individual becomes. Considering that measure in terms of risk measurement, each instance of personal information released by the individual or by a third party, can therefore be seen in terms of increasing the risk. Risk measurement, risk assessment and risk management techniques can therefore be applied to control the amount of personal information and thus reduce the risk.

Reducing the risk links well with the approach advocated by Clarke (1995) in Situational Crime Prevention (SCP). SCP is where the opportunity for specific categories of crime are reduced. This looks primarily at offender reactions in different situations where the risk of being caught or convicted is high, then the benefits of committing the crime have to be high for them to offend. The Internet combined with the anonymity provided by some PETs has enabled the abuse of information to happen with reduced risk detection.

Current PETs do fit into this situations of risk assessment, or management. Young people wish to share their information with others for social networking purposes and will circumvent various filtering controls and constraints; personal information has to be divulged during certain transactions; government public records are published; many situations have an unequal power balance against the individual, there are no other real alternatives but to give out the information. Therefore PETs that rely on making individuals choose between anonymity or identity are not suitable, they do not fit this context.

If the approach is taken whereby technology enables and empowers the individual to take more responsibility for their actions, a reduction in risk should follow. This approach is seen with the current health and safety approach in this country. The UK Government has enacted legislation to enforce safe practice within the workplace, The Health and Safety at Work Act, 1974; business and employers have a duty of care to their workforce and to their customers; and individuals have a duty to act in ways that continue that duty of care to both themselves and to others.

PETs could be created to combine the monitoring of the release of personal information in such a way that individuals had control over it, they could return to where they gave out the information and perhaps be able to take steps to remove it should they wish. Personal information held by other

parties could also be monitored. This approach needs to be embedded into everyday tools which are intuitive and easy to use, that do not require very much in the way of mental overhead for the individual.

To achieve this approach, the next phase in this research is to create a prototype browser plug in that allows individuals to keep track of where they have given out their personal information, where information is stored about themselves and links to current advisory sites to help them make decisions.

6 Conclusion

The findings from the two groups has illustrated the different risks that occur from the release of personal information. Readily available tracking technologies; release of personal details; divulgence of information by third parties all combined causing different threats. In the case of Survivors, often the impacts were felt even though they did not themselves engage with the technologies.

Teenagers made good use of the web in a predominantly social manner. The use of messenger and social networking websites illustrated a significant amount of personal information being divulged. Teenagers demonstrated their proficiency at making use of the software controls provided or by providing false information to circumvent excessive collection of personal data.

To address the current criticisms of PETs technological solutions need to allow individuals the ability to minimise their risks, that are intuitive and relevant to the situation in which the individual finds themself. In this regard, PETs could then be seen to fulfil a role in controlling the risks for the potential for harm.

The purpose of this research has been to explore the privacy issues faced by the more vulnerable members of society. The issues highlighted in the study where individual's have been exposed to a risk of harm, or where privacy has been eroded through an individual's own use, or another's use of technology, form important elements for consideration when considering the impact of technology upon privacy. These useful pointers can be used by designers of technology and software; for policy-makers and for those who have a moral responsibility for individuals.

Future work will involve a study of how technology may combine with other social and human factors to bring about a reduction in the elements of risk faced by the two vulnerable groups used in this study.

7 References

Abrahams, H, (2007), *Supporting Women after Domestic Violence*, Jessica Kingsley, London.

BBC News, (2006), "*Privacy fears hit google search*", 10th February 2006, http://news.bbc.co.uk/1/hi/technology/4700002.stm (accessed 30 November 2006)

Bocij, P, (2004), *Cyberstalking*, Praeger, Conneticut

Burkett, H, (1997), "Privacy-Enhancing Technologies: Typology, Critique, Vision", In Agre, P.E., and Rotenberg, M (Eds), *Technology and Privacy: The New Landscape*, MIT Press, London

Cannon, J.C., (2004), *Privacy What Developers and IT Professionals Should Know*, Addison Wesley Professional, Harlow

Caspian (2004), "Consumers against supermarket privacy invasion and numbers", www.nocards.org, (accessed 31 March 2007)

Clarke, R.V., (1995), "Situational Crime Prevention, Building a Safer Society: Strategic Approaches to Crime Prevention", *Crime and Justice*, Vol. 19, pp. 91-150

CRU, (2006), *Internet Safety Zone*, Cyberspace Research Unit, University of Lancaster http://www.internetsafetyzone.co.uk/root/default.htm (accessed 30 November 2006)

Dahlberg, L., (2004), "Internet Research Tracings: Towards Non-Reductionist Methodology", *JCMC*, 9 (3) April 2004, http://jcmc.indiana.edu/vol9/issue3/dahlberg.html (accessed 30 November 2006)

Dinev, T. and Hart, P, (2004), "Internet Privacy Concerns and their Antecedents - Measurement Validity and a Regression Model", *Behaviour and Information Technology*, Volume 23, Issue 6, November 2004 pages 413-422

European Commission, (2006), *Safer Internet Programme*, Europe's Information Society, http://europa.eu.int/information_society/activities/sip/index_en.htm (accessed 30 November 2006)

Feenberg, A, (1999), *Questioning Technology*, Routledge, London

Fiveash, K, (2006), "Internet safety talks for UK kids", *The Register*, http://www.theregister.co.uk/2006/09/20/internet_children_safety/ (accessed 30 November 2006)

Furnell, S, (2005), "Internet threats to end-users: Hunting easy prey", *Network Security*, July, pp5-9

Fraud Advisory Panel (The), (2005), *The Human Cost of Fraud: Seventh Annual Review*, Fraud Advisory Panel, http://www.fraudadvisorypanel.org/newsite/Publications/Publications_annualreports.htm (accessed 30 November 2006)

Garfinkel, S, (2000), *Database Nation*, O'Reilly Associates, Sebastopol, CA

Givens, B, (2000), "Eight Reasons to be Skeptical of a "Technology Fix" for protecting privacy", In *Proceedings of Computer Professionals for Social Responsibility*, University of Pennsylvania, Philadelphia, http://www.privacyrights.org/ar/8skeptical.htm (accessed 30 November 2006)

Goldberg, I, (2003), "Privacy-Enhancing Technologies for the Internet, II: Five Years Later", In *Privacy Enhancing Technologies*, LNCS Volume 2482/2003, Springer Berlin / Heidelberg

HiSPEC, (2002), "Privacy Enhancing Technologies State of the Art Review", www.hispec.org.uk, http://www.hispec.org.uk/public_documents/7_1PETreview3.pdf (accessed 30 November 2006)

Home Office, (2006), "Child Exploitation and Online Protection Centre", http://www.ceop.gov.uk/ (accessed 30 November 2006)

Hughes, D.M., (2003), "Prostitution online", *Journal of Trauma Practice*, Vol 2. No 3/4, 2003, pp115-132 http://www.uri.edu/artsci/wms/hughes/internet.pdf (accessed 30 November 2006)

Magid, L, (2004), "Teen Safety on the Information Highway", *National Center for Missing and Exploited Children*, http://www.safeteens.com/safeteens.htm#Guidelines_for_Parents_0 (accessed 30 November 2006)

Margulis, S.T, (1977), "Conceptions of Privacy: Current Status and Next Steps", In *Journal of Social Issues*, 33. 5-10

Mitchell KJ, Finkelhor D, Wolak J, (2005), "The Internet and family and acquaintance sexual abuse", Child Maltreatment, 10 (1): 49-60 FEB 2005

Mitnick, K. D.,Simon, W. L., (2003), *The Art of Deception: Controlling the Human Element of Security*, Wiley

No2ID (2007), "The NO2ID Campaign", www.no2id.net, (accessed 31 March 07)

Raab, C.D and Bennett, C.J, (1998), "Distribution of Privacy Risks: Who Needs Protection", *Information Society*, Vol 14, Issue 4, p 263-274

Raab, C.D., (2004), "The Future of Privacy Protection", *Cyber Trust and Crime Prevention Project*, http://www.foresight.gov.uk/Previous_Projects/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/The_Future_of_Privacy_Protection/The_Future_of_Privacy_Protection.html (accessed 31 March 2007)

Solove, D.J, (2004), *The Digital Person*, New York University Press, New York

Southworth, C., Dawson, S., Fraser, C., Tucker, S., (2005), "A High Tech Twist on Abuse: Technology, Intimate Partner Stalking and Advocacy", *Violence Against Women Online Resources*, Minesota http://www.mincava.umn.edu/documents/commissioned/stalkingandtech/stalkingandtech.html (accessed 30 November 2006)

Spychips (2007), "RFID 1984", www.spychips.com, (accessed 31 March 2007)

The Big Opt Out (2006), "NHS Confidentiality Campaign", www.nhsconfidentiality.org, (accessed 31 March 2007)

Ward, M, (2006a), *Radio Tag Study revealed at Cebit*, BBC, 10th March 2006, http://news.bbc.co.uk/1/hi/technology/4792554.stm (accessed 30 November 2006)

Ward, M, (2006b), *Wi-fi set to re-wire social rules*, BBC, 8th March 2006, http://news.bbc.co.uk/1/hi/technology/4770188.stm (accessed 30 November 2006)

Wired News, (2006), *Teens Reveal Too Much Online*, Associated Press, 5th February, 2006 http://www.wired.com/news/wireservice/1,70163-0.html (accessed 30 November 2006)

Womens Aid Federation of England, (2002), *Domestic Violence Statistical Factsheet 2002*, , http://www.womensaid.org.uk/dv/dvfactsh2002.htm