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 inviduals 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).

3.1 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.

4.1 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.

4.1.1 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."

4.1.2 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."

4.1.3 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:

- personal information was freely divulged by the residents about themselves and about other residents.
- 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."

4.2 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.

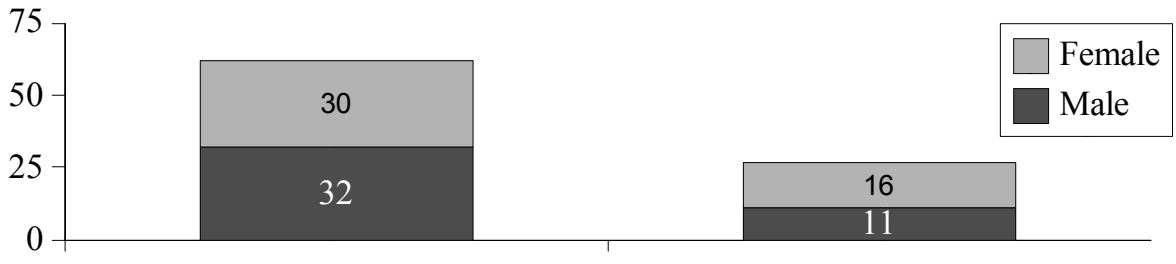

Figure 1: Gender split on divulging Personal Information

4.2.1 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.

4.2.2 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 explicilty 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 inutuitive 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 policymakers 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.

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