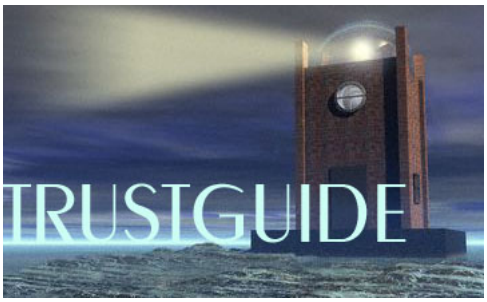

www.trustguide.org.uk

Trustguide: Final Report

October 2006

Hazel Lacohée

BT Group Chief Technology Office, Research & Venturing

hazel.v.lacohee@bt.com

Stephen Crane

HP Labs

stephen.crane@hp.com

Andy Phippen

University of Plymouth, Network Research Group

andy@jack.see.plymouth.ac.uk

Rev: 20 November 2006

In association with

http://www.knowledgewest.org.uk

www.network-research-group.org

Executive Summary

Trustguide is a collaborative research project between BT Group Chief Technology Office Research and Venturing and HP Labs, part funded by the DTI Sciencewise programme. The research seeks to build on the previous government sponsored Foresight project[1] concerned with where responsibilities lie in making our future ICT-enabled world safer. The objectives are:

- To establish a dialogue between those that use and shape technology to enhance cyber trust
- To produce and champion guidelines for those engaged in the research, development and delivery of ICT on how cyber trust might be enhanced

Trustguide takes a "citizen-centric" approach to understanding the beliefs and needs of users in relation to trust, security and privacy in ICT mediated activities. It has established a dialogue with the public through facilitated focus group discussions among selected groups across the UK. Topics covered in these groups include:

- Trust versus risk
- E-Commerce: Risk and Responsibility
- Factors that impact on risk taking
- Mitigated risk
- ID cards: An aid to security?
- Use of Biometric data
- Privacy and health information
- E-Government and Public Sector IT
- Awareness and education
- Use of public access terminals

While there are a number of different issues presented within the report, there is one cross cutting theme that emerges. While an initial hypothesis may be that people do not engage with online services because they do not *trust* them, our findings have shown that trust is not as significant a measure as first thought. What is more important to understand is that people are willing to take risks online, as long as they are informed, and it is clear how consequences will be addressed. People use specific services not because they *trust* them, but because they in some way provide a benefit to the individual and they know that if something goes wrong, restitution will be made.

The data collected through Trustguide has enabled the development of a set of guidelines to inform policy making and service development for ICT mediated services:

Education - Enabling better-informed risk decision-making. The fundamental foundation of the guidelines lies in education. Citizens engage with services because they make a decision concerning whether it is worth the risk to engage (i.e. do the pros outweigh the cons). Currently education is sparse and disconnected, resulting in ill-founded beliefs hampering engagement. A more educated online society is more likely to engage with ICT mediated services based upon confidence through knowledge.

[1] The Foresight Cyber Trust and Crime Prevention project, http://www.foresight.gov.uk/previous_projects/cyber_trust_and_crime_prevention/index.html

Experimentation – Learning through doing. Complementary to education, people will develop trust in a service through experimentation in a "safe" environment prior to engaging in a potentially risky transaction.

Restitution Measures – Provide a positive impact on personal perceived risk. Citizens believe there is no such thing as a secure service and claiming so leads to mistrust. A more effective method of engagement is to clearly state the measures that are in place in the event of something going wrong.

Guarantees – Provide assurance and improve confidence in whether to enter into a transaction through guarantees of restitution. Guarantees should be open and honest, and suitable in aiding an individual in making an informed choice regarding whether to engage with a new service.

Control – Increased transparency brings increased confidence. Citizens are aware of large-scale data collection through online services and mistrustful of it. They know it is *their* data, and they want to be able to control it.

Openness – trust is not built through unsubstantiated claims of security and protection. Being clear about the benefits and issues related to a service will engender far greater trust.

We present compelling evidence that challenges current thinking on how to engage individuals with ICT mediated services. People are sceptical about technology, and rightfully so. However, if empowered and allowed to experiment, they tend to adopt solutions that are socially beneficial. The changeover will not happen overnight, but it should be driven by people's ability to correctly ascertain the extent of trust they can extend towards technology. Education and assurance are the foundation stones upon which trust is built and understanding the risk-trust-privacy-responsibility-restitution equation is fundamental to increasing confidant use of ICT mediated services and emerging technologies. These problems will require constant and meticulous research if we are to achieve Government's vision of everyone in our country confidently enjoying the benefits that increased use of ICT can undoubtedly bring. We need to understand the issues of today and those that may arise in the near and more distant future and we must ensure that we address the most appropriate research questions and gaps in understanding

We can conclude that security is neither a trivial nor a static problem and cannot be treated as a separate or distinct issue from trust given that it is intrinsically linked to the issues that impact on adoption, acceptance and confidant use of both new and existing technologies. Mobile technologies, pervasive computing, broadband etc. bring many challenges not only to managing security or reliability as such, but first and foremost, to the perception of how trustworthy a system actually is. 'Doing security properly' in order to enhance trust and privacy concerns is simply no longer sufficient. Trust is a construct that calls for interdisciplinary research. We feel that a fruitful way forward to ensure that we are addressing the most relevant and appropriate research questions is to draw together a community of people from different backgrounds and disciplines to work on this together so that we can employ different sources of expertise including security, community, and social scientists.

Contents

1 Introduction to Trustguide

Trustguide[2] is a collaborative project between BT Group Chief Technology Office Research and Venturing and HP Labs that builds on the findings of the Foresight Cyber Trust and Crime Prevention Project[3]. The Foresight Cyber Trust and Crime Prevention project began a dialogue into where the responsibilities lie in making our future ICT-enabled world safer and this debate has now been extended to include the public. BT and HP both have extensive experience of developing technology from research through to product and services, in testing that technology with the public and routinely supporting the wider involvement of the public with science, and so present a worthy partnership to undertake the Trustguide project.

The Trustguide project is funded in part by the DTI Sciencewise programme[4]. Sciencewise supports projects that bring together scientists, government and the public to explore the impact of science and technology in our lives. The Sciencewise initiative was launched by Lord Sainsbury at the BA Festival in September 2004 with the aim of building public engagement in order to explore the many implications that may be of concern in emerging technologies. The Government wants the UK to take full advantage of the opportunities offered by scientific discovery and technological development and aims to build societal confidence in the decisions that are made in the development, governance, regulation and use of science and technology. To achieve this, the Government believe that the public should be given the opportunity to engage in dialogue about the ethical, safety, health and environmental implications of new areas of science and technology. The reasoning behind this is very clear; how we adopt and use technology is seen by Government as crucial to the nation's future prosperity. Government is committed to ensuring that[5]:

> *"…Everyone in our country has the opportunity to benefit from the transformative power of ICT."*

And part of that vision entails:

> *"Creating a country at ease in the digital world, where all have the confidence to access the new and innovative services that are emerging, whether delivered by computer, mobile phone, digital television or any other device, and where we can do so in a safe environment."*

Trustguide is concerned with exploring issues of trust, security and privacy in ICT based applications and services via a series of workshops and discussion groups that cover as broad and appropriate a spectrum of the UK's citizens as the scope of the project allowed. The aim of the project is to use this dialogue and its outputs to establish recommendations and guidelines for the research, development and delivery of trustworthy ICT and to inform the policymaking processes used by government, industry and other key organisations. From BT's perspective Trustguide demonstrates the effectiveness of using advanced technology to provide an effective method of accessing customers' perceptions about these issues Since we have applied a fluid methodology that builds upon the findings of each workshop it also enabled us to introduce topics for discussion that were not raised at the beginning of the project. This flexibility allowed us to be responsive to current and evolving research initiatives. The project has also enabled us to maximise and build on our relations with the

[2] Trustguide, http://www.trustguide.org.uk/

[3] http://www.foresight.gov.uk/previous_projects/cyber_trust_and_crime_prevention/index.html

[4] Sciencewise, http://www.sciencewise.org.uk

[5] March 2005 Connecting the UK: the Digital Strategy. Cabinet Office, Prime Minister's Strategy Unit, joint report with the Department of Trade and Industry.

University of Plymouth's Network Research Group[6] who have a long established track record in the research of information systems security and have a growing interest in the socio-technical implications of technology. The Trustguide project provides an unparalleled opportunity for studying a topic in a way that would be very difficult to achieve through traditional academic routes. The work of Trustguide compliments other work the group is carrying out related to the public perception of IT, the usability of end-user security products, and citizen engagement and e-democracy. The group have contributed to the methodology, data collection and analysis within the project, and are also able to exploit academic links in order to disseminate project findings to an academic audience.

HP recognises that introducing any technology can create dilemmas, particularly where security is concerned. Balancing ease of use against feature-sets designed to protect privacy and engender trust is a responsibility that is taken very seriously, from early research through to deployment. Understanding why negative experiences of trustworthiness arise, and how they should be addressed is key to the successful introduction of technologies that are true enablers of the digital world. HP recognises that this challenge is not simply the responsibility of technology innovators; legislators, policy makers and society in general influence and are influenced by national demand for innovation. Trustguide has provided an excellent and welcomed opportunity to understand these tensions at first-hand, particularly where the project engages with the public in the context of existing and on-going technology research.

To summarise, the objectives of the Trustguide project are:

- To build on the outputs of the Foresight project
- Establish a dialogue between those who shape the technology, other interested participants, and the wider public, in order to enhance the existing cyber trust community so that it is capable of addressing complex and subtle issues as they arise
- Produce guidelines for those engaged in the research, development and delivery of ICT on how cyber trust might be enhanced
- Champion the guidelines

[6] University of Plymouth's Network Research Group, http://www.network-research-group.org/

2 Achieving engagement with the public

Both the Foresight[7] and Royal Society[8] projects found it difficult to get participants into a frame of mind where they could see how technology might develop and the implications that this might have upon trust and security. Trustguide has overcome this by employing advanced technology and current topical media stories to stimulate debate and discussion.

We engage participants of each workshop in one or more current research projects concerning advanced future technologies that have been developed to proof of concept stage in our Labs. This creates an interactive hands-on experience for participants with lab prototypes that require engagement with trust, security and privacy issues in a novel way that would otherwise be outside of their experience (an example of one of the projects we have employed is shown in Appendix A.1). We have chosen prototypes that create tensions between trust and privacy issues and have designed the demonstration process to be undertaken in an informal manner that creates a relaxed environment where questions can be asked and discussion can take place. This provides an appropriate introduction and backdrop to the rest of the workshop where a semi-structured discussion takes place that explores these issues in greater depth and breadth. This is described in more detail in the following section but is designed to cover the following areas:

- Establishment of identity is important for trust in e-commerce
- Establishment of identity requires data gathering
- Different types of data are perceived as more or less private
- Data gathering as a perceived threat to privacy
- Trust in organisations gathering data

By employing advanced technology to stimulate debate and discussion we are not only able to overcome the problems of engagement experienced by previous projects, but are also provided with an opportunity to gather feedback on our prototypes that further aids the on-going development of the concepts we demonstrate.

2.1 Workshop structure and content

The aim of the workshops is to produce qualitative data in order to develop hypotheses that can be tested and explored in finer detail in future studies. Since we are concerned with public engagement and attitudes to the issues described above we wanted to cover as broad and appropriate a spectrum of the UK's citizens as the scope of the project allowed. Knowledge West[9] has assisted us in recruiting attendees at some of the workshops in the West by establishing connections with public, SME and expert groups.

We have conducted 29 workshops with the following groups:

- Students
- General public
- Farmers
- SMEs

[7] Foresight "Cyber Trust and Crime", http://www.foresight.gov.uk/previous_projects/cyber_trust_and_crime_prevention/index.html

[8] Royal Society, "Cybertrust and Information Security," http://www.royalsociety.org/page.asp?id=1987

[9] Knowledge West, http://www.knowledgewest.org.uk/index.asp

- Expert groups (corporates, academics and researchers engaged in this area)
- ICT novices
- E-Gov service providers
- Schoolchildren

As shown above, in addition to the groups carried out with adults we also carried out a number of groups with schoolchildren ranging from year 8 to year 11 in schools in the South West. It was important to consider the opinions of younger people within our dialogue as they, firstly, form the basis of the next generation of ICT service producers and consumers, and secondly, already make up a large part of the online audience targeted by service providers.

The method used for dialogue with schoolchildren was similar to the adult groups (facilitated semi-structured discussion) but the approach differed. In the case of schoolchildren it was more appropriate to work with smaller numbers in each sample and we have completed ten groups in this segment with a total of 97 participants. The method for our work with schoolchildren was adopted from one designed by a Ph.D. student within the Network Research Group at the University of Plymouth and the discussion guide is provided in Appendix A.3. Participants were initially asked to fill out a questionnaire to get them thinking about their use of the Internet and were then presented with scenarios for discussion. The results specific to these groups are detailed in section 9.

We also wanted to have a comparison point between novice and expert groups and included a group of novice ICT users for this purpose.

We have attempted to cover as a wide a geographical area as the constraints of the project allowed and in total we have completed 29 workshops (300 attendees) with groups across the following locations:

Type of group	Location
1. Undergraduate students – these were an initial pilot group to ensure effective structure for the subsequent discussions. However, this was treated as a full group discussion – all the students were in the final year of undergraduate courses in computing, so would have a good depth of technical awareness, although their knowledge might not have been security-specific.	Plymouth
2. Postgraduate students – an effective comparator to the undergraduate group, this was a group on a specialist MSc Information Systems Security programme and therefore should have a more thorough depth of knowledge around the issues of trust and security (note: the participants were approximately one term into their study at the time of the focus group).	Plymouth
3. SME employees – employees drawn from IT SMEs – all were technically aware and were in the business of providing ICT services, as well as carrying out business online. Hence they were expected to have opinions from both perspectives in the trust relationship.	Bristol

Type of group	Location
4. Citizens – members of the public, recruited via local press advertising. The aim was to obtain a more general public perspective, but it is acknowledged that people responding to such adverts generally have a vested interest in the subject matter for discussion, and this was borne out, as the group was possibly more IT aware than a random cross section.	Bristol
5. ICT Novices – participants drawn from a community group that had been formed to provide very basic IT training in a relaxed informal environment. Generally, but not exclusively, based upon an over 50s population.	Helston, Cornwall
6. Farmers – the inclusion of a group of farmers may appear to be somewhat incongruous but they were chosen because the UK Government has recently set up a strategy (November 2005[10]) to design services across central and local government boundaries and between departments for particular groups of customers, focusing initially on farmers (and also the elderly, and offender management.)	Wadebridge, Cornwall
7. SME – e-commerce start-ups - a group of SMEs from a variety of commercial sectors, all were on an e-commerce adoption path as a result of work with Cardiff University's e-Commerce Innovations Centre. An interesting group as they were trying to engage with technologies to enhance their businesses without being particularly technically able.	Cardiff, Wales
8, 9 and 10 SME start ups – three groups of SMEs within the first year of business, a split of IT companies and companies that consumed IT services as part of their business.	Swindon, Bath, Bristol
10. Expert – a group of individuals from different domains, each with many (10+) years experience within the technology field (including a company director with experience of directing a large UK ISP, a company director with experience in an enterprise technology sector and an advisor to the Foresight programme, an academic with experience in the web technology and security field, and a business advisor with experience of advising start up companies on technology solutions).	Bristol
11. Citizens – general public, recruited in the same way as described above.	Bristol

[10] http://www.cio.gov.uk/transformational_government/strategy/index.asp

Type of group	Location
12 and 13. Postgraduate students – Royal Holloway College and LSE. Royal Holloway students were a group of post grads studying for PhD in information security. The LSE group represented mainly psychology students. This group presented an interesting juxtaposition to the earlier, technology focused students, allowing investigation of a greater breadth among the student community.	London
14. Experts – a group of academics and recognised experts involved in security research and teaching, drawn from colleges of London University (UCL, Imperial, RHUL, LSE).	London
15 - 25. Youngsters – schoolchildren representing years 8 and 11 from various schools across South Devon enabled an exploration of the attitudes of the up-coming generation of citizens and, arguably, one of the more technologically aware demographic groups.	South Devon
26. Local Government – a group representing North Cornwall District Council involved in policy setting for a wide range of public facing services, including heath, leisure, planning, housing and social services. This group enabled us to examine attitudes from the service provision/delivery viewpoint, which gave balance to the majority of our groups that were from the demand, rather than supply, side of the ICT service relationship.	Cornwall
27. Open University – a group of philosophy students attending residential Summer School. They were mature students with a broad set of personal experiences and representing a wide age range, again, giving greater breadth to our range of students surveyed.	Bath
28. Professional body representatives – a group of members, typically chartered status, representing the Institution of Engineering and Technology (formally the Institution of Electrical Engineers) and the British Computer Society. The group included mostly people from leading organisations involved in the development or application of communications and computer technologies.	Bristol
29. Researchers – researchers in security from HP's corporate research labs. This group attended the last workshop to be conducted and in addition to contributing their expertise provided a commercial viewpoint on service delivery which complimented the views of those from the public sector	Bristol

The semi-structured discussions were professionally facilitated and covered relevant topic areas that were identified via the outputs of the Foresight project and a wider literature search:

- Awareness and education in ICT mediated activities
- Establishing identity

- Current and future means of identification and authentication processes (including biometrics and ID cards)
- Identity management, theft, and fraud
- Data storage, collection, security and privacy
- Trust and use of online services including e-Government and e-commerce
- Trust in organisations gathering private data

Figure 1 illustrates the model we employ for the workshops:

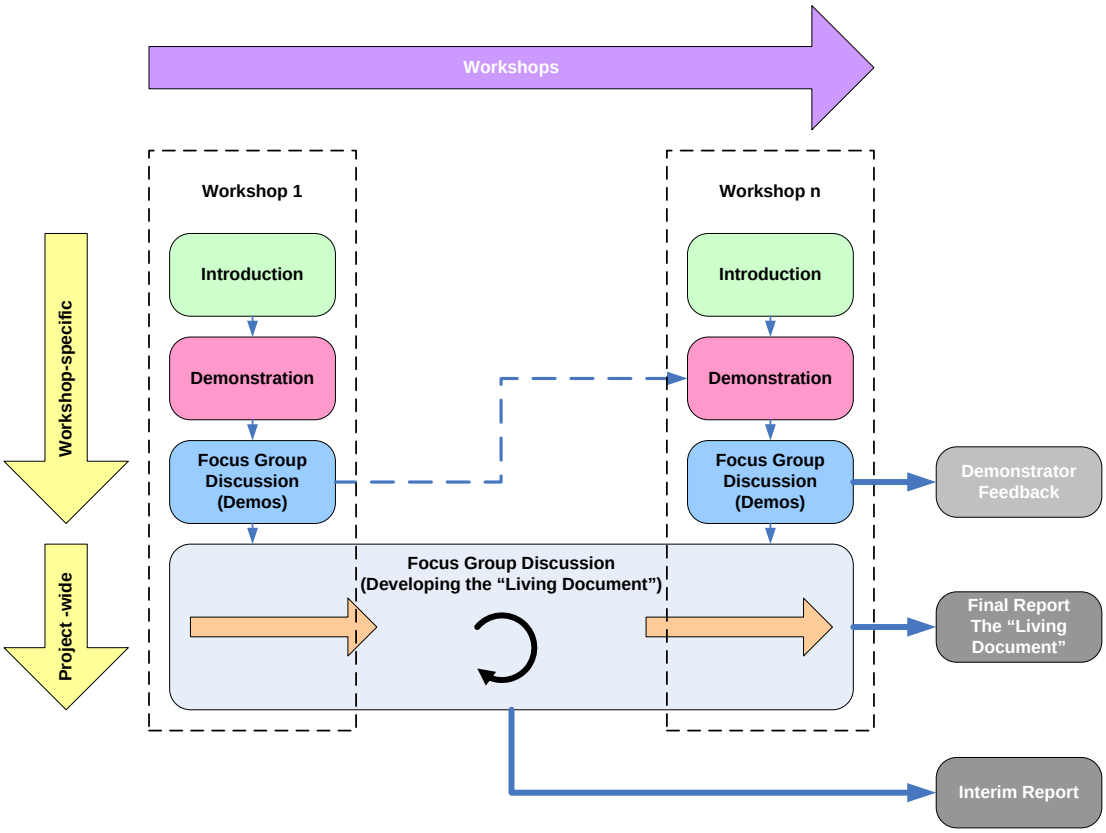

Figure 1: Schematic workshop model

2.2 Building a living document

By taking the outputs of Foresight as the starting point, each workshop sought to refine a living document that builds into an appropriate set of recommendations and guidelines. In addition to the workshops the project also used a web site and on-line discussion forum[11] to give workshop participants an opportunity to monitor and contribute to the progress of the project. Membership of the forum was restricted to those who had attended a workshop, and typically on-line discussions started where a workshop ended. Topics were introduced to seed a particular discussion point, and to introduce current events (e.g. news items) that related to topics we had discussed, but presented a different angle or attitude. Each workshop had its own discussion area, but all participants were encouraged to contribute to discussions that arose from or after other workshops. The creation of the forum not only enabled attendees to maintain their engagement with the project, it also allowed them to continue to contribute to

[11] https://www-apps.hpl.hp.com/trustguide/index.php

the development of the guidelines. Examples of topics discussed include: brand loyalty, banking, health, and e-Government services.

We recently exhibited at the InfoSecurity[12] event where we also extended our forum facility and launched a public on-line discussion forum and questionnaire[13].

In addition, our association with the University of Plymouth has also enabled us to access a public facing questionnaire[14] they have produced that explores attitudes to the issues of trust, privacy and security complimentary to those we discussed in the workshops. This survey was aimed at a wide population and disseminated using a viral approach to ensure breadth of coverage.

Accessing this data, with a high level of respondents, allowed us to reach the opinions of a larger population than was possible solely with the focus groups. While the data collected is not as rich as that collected within the discussion activity, it does allow a breadth of coverage that compliments the depth that is provided through the groups. This mixed methodological approach, using a combination of qualitative and quantitative data, enables greater validity and generalisability of our findings and adds richness to the project outputs. Key findings from this survey are detailed in Appendix A.4 and the implications of these findings related to the Trustguide evidence are discussed in section 8.1.

2.3 Data collection and analysis

All workshops were recorded; discussion groups were run by a professional facilitator to engage and guide discussion and comprised at least one observer to take notes. Observers' notes enabled the recording of non-verbal data (for example, attendees' reactions to a topic or technology, show of hand counts for questions, etc.).

Attendees were assured of the anonymity of the group prior to the start of discussion and their permission was sought to record the discussion. All attendees in all groups, bar one individual were happy with this and the discussions were recorded for later transcription.

Transcripts and observers notes were coded to a common scheme (see Appendix A.2) and analysed using QSR N6, a qualitative data management and analysis code-based tool for use with open-ended survey data, in depth interviews and focus group transcripts. In depth analysis of the transcripts is presented in the body of the report with relevant quotes to illustrate the points made.

Attendee quotes are presented in the body of the report as demonstrations of opinions in relation to different topic areas. One of our most significant findings was the similarity of opinions across all groups and we have deliberately chosen not to identify quotes in terms of particular groups except where pertinent to do so. Given the nature of the semi-structured discussion process some groups spent more time on particular topics than others but this tended to occur because someone in that group wanted to share a particular experience or because there had been recent media coverage rather than a particular topic being more relevant to one group than another. Hence identification is only made where it is relevant and/or adds to any insights or inferences that may be drawn.

[12] InfoSecurity is the leading exhibition for the UK information security industry, held annually at Olympia in London. http://www.infosecurityevent.com

[13] https://www-apps.hpl.hp.com/trustguide/questionnaire/

[14] http://www.securityperceptions.net/

3 What do we mean by 'trust?'

In the context of ICT use, and in particular e-commerce, e-Gov, and health, the creation, maintenance and enhancement of trust is of primary concern to those involved in the successful design, development and implementation of ICT based applications and services. Indeed, trust makes cooperation possible and is widely held to be the foundation of human communication and interaction[15], but what do we mean when we talk about trust? Basically trust presents a semantic problem; trust is a broad construct that has numerous definitions and meanings across multiple disciplines including economics, psychology and sociology and of course, each of these views trust from its own particular perspective. Even dictionaries cannot agree[16]; three unabridged versions (Websters, Random House, and The Oxford English Dictionary) give nine, twenty-four and eighteen definitions respectively. Whilst some psychological perspectives of trust take the view that it is a personal characteristic based on choice, more generally social science defines trust as 'an attitude of positive expectation that one's vulnerabilities will not be exploited[17], and dictionary definitions include '…a firm belief in the reliability or truth or strength etc. of a person or thing…a confidant expectation…and reliance on the truth of a statement etc. without examination.' Consequently there are a significant number of models of trust. Those models however tend to take either the sociological (e.g. Interpersonal/ Dispositional trust), or technical approach[18] (trust as subjective probability e.g. computer network security, agent-based commerce) and we favour the recently developed complexity-based model of confidence[19] that demonstrates a more interdisciplinary approach.

There is no doubt that trust is of central and significant importance to commercial relationships, or indeed any relationship where there is risk, uncertainty or any degree of interdependence. In the context of ICT mediated activities the concept of trust is even more complex because we are operating in an environment where perceptual information available in face-to-face, and to a lesser degree in telephone transactions, upon which we partly base our trust decisions, is entirely absent. It is also worth noting that in this context many people are engaging with technologies and operating within an environment that they do not understand and while this increases the level of difficulty that they may experience it also highlights the need for better education and understanding so that they can make better-informed decisions.

3.1 Trust versus risk

One of the objectives of our research is to understand how cyber trust might be enhanced; a sensible starting point might be to tease out which ICT mediated services and technologies more generally are considered most trustworthy, what signifies that trustworthiness, and why. A wealth of research has focused on this perspective, from the all-encompassing aspects of

[15] Niklas Luhmann. Trust and Power. Wiley, 1979

[16] 2001 D. Harrison McKnight & Norman L. Chervany. Conceptualizing Trust: A Typology and E-commerce Customer Relationship Model.

[17] Rousseau, D.M., Sitkin, S.B., Burt, R.S., & Camerer, C. Not so different after all: A cross discipline view of trust. Academy of Management Review 1998. 23 (3), pp393 -404

[18] A. Abdul-Rahman: A Framework for Decentralised Trust Reasoning. PhD thesis, 2005. http:// www.cs.ucl.ac.uk/ staff/ F.AbdulRahman/ docs/ thesis-final.pdf

[19] Piotr Cofta: Complexity, trust and control: the model of confidence. In: Confidence in a convergent world: trust, complexity and control (in prep.)

how to build trust and confidence in the complex environment of pervasive systems[20], to maximising perceived trustworthiness in e-commerce[21], communicating trustworthiness in web design[22], and determining factors that influence customers' trust in online businesses[23]. HP has also conducted research in this area in the context of how technology may provide the link between human perception and a highly technical world[24], and the tensions between trust and technologies considered to be trustworthy in analyses of restaurant customers' attitudes to different payment methods[25]

However, one of our most significant findings is that it very quickly became apparent that this might not be the most fruitful or appropriate line of enquiry for our research. We found a high degree of distrust of ICT mediated applications and services. Workshop attendees repeatedly informed us for example that they believe that it is impossible to guarantee that electronic transactions or electronically held data can be secure against increasingly innovative forms of attack:

> *"The real issue is that we know from our experience of the Internet and everything else that nobody has ever yet made anything secure. Whatever kind of encryption you've got, it can be broken."*
>
> *"No system can be secure because it's got all these people on the other side sitting in front of terminals. Even if the data was electronically secure at the front end it can't be secure at the back end."*
>
> *"I think it's important to remember that any fraud prevention system works for a while and then criminals find a way round it."*

Also, attendees reported that as more data is gathered and stored electronically, particularly in central databases, and the more they use ICT mediated services, the more vulnerable they feel. The comments below typify attendee attitudes:

> *"I think in the electronic world there could be an awful lot more people who are attempting to get at your data so that makes you more at risk."*
>
> *"We know that no one has ever built a secure system, nothing held electronically can be secure. Banks (etc) should be more honest and say that data is never secure, and they should be open about the risks."*

However, this commonly held belief does not inhibit use of the many ICT mediated services available, in fact quite the contrary. Our project shows that it is not trust per se that should be

---

[20] J. Clarke, S. Butler, C. Hauser, M. Neubauer, P. Robertson, I. Orazem, A. Jerman Blazic, H. Williams, Y. Yang: "Security and Privacy in a Pervasive World", EURESCOM Summit 2005, Ubiquitous Services and Applications – Exploiting the Potential, Conference Proceedings, 27-29 April 2005, Heidelberg, Germany, VDE Verlag, Berlin, Offenbach (ISBN 3-8007-2891-5), pp. 315-322.

[21] D. Harrison McKnight, Norman L. Chervany: The Meanings of Trust. In: University of Minnesota, http://www.misrc.umn.edu/wpaper/wp96-04.htm. 1996.

Yao-Hua Tan, Walter Thoen: Formal Aspects of a Generic Model of Trust for Electronic Commerce. In: Proceedings of the 33rd Hawaii International Conference on System Sciences - 2000

[22] Nielsen, J.1999. Trust or Bust: Communicating Trustworthiness in Web Design. http://www.useit.com/alertbox/990307.html

[23] Shore 2001: Ceaparu, I., Demner, D., Hung, H., Zhao, H. "In Web we Trust": Establishing Strategic Trust Among Online Customers. http://www.otal.umd.edu/SHORE2001/webTrust/index.html

[24] Cofta, P. & Crane, S. Towards the Intimate Trust Advisor, iTrust 2003, Greece

[25] HP Labs Technical Report, HPL-2004-113: Security and Trust in Mobile Interactions: A Study of Users' Perceptions and Reasoning 2006-06-04

at the forefront of research, rather it is the perceived risks and associated decision making processes that users are prepared to undertake in order to avail themselves of the advantages that technological advances afford that are worthy of a good deal more attention. Not that this makes the task in hand any easier; the concept of what constitutes a risk, and under what circumstances, is open to as many definitions and interpretations as the concept of trust. However, it is interesting to note that attendees commonly referred to 'risk' rather than 'trust' when describing their ICT mediated experiences and that they tended to focus on fraud and theft of credit card details even though the discussion process left them free to explore any avenue in relation to this topic:

> *"If it's a necessity to do something then you'll take the risk - I bought tickets for something off a site in an Internet café. I didn't feel comfortable about doing it but it was the only way to get the tickets."*

> *"I think it's true with e-banking and it's true with buying things online, it's just so convenient that people are prepared to take the risk, unless it got completely out of hand, I think people are prepared to take that risk."*

> *"For each of those situations it's a judgement call, is it worth the risk or not, do you feel happy with it or not? You try and reduce the risk as much as you can without reducing any kind of fun as much as you can."*

In evaluating the concept of risk we asked workshop attendees whether they felt more or less at risk of becoming the victim of cyber crime compared with the potential for being a victim of crime in the physical world. Somewhat surprisingly none of the attendees mentioned the wider variety of crimes that we might fall victim to in the physical world but there was also no consensus as to whether one is more or less at risk in the cyber world:

> *"There are always ways and means, whether it's by phone or mail, or handing your card over or whatever, it can be misused. There's always a risk, it's no more risky to use your card on the Internet than elsewhere really."*

Some felt that there was more chance of being a victim of cyber crime:

> *"I think I'm far more likely to be the victim of cyber crime, that's purely from experience; I do more things electronically than physically and so there are all sorts of ways that could happen. If you just look at the amount of phishing emails I get for example, they're not going to catch me out but they could if I wasn't concentrating perhaps."*

> *"In the real world, if you're in a restaurant you've only got three or four waiters who potentially might be corrupt, and you'd soon know if they were stealing credit card details on a regular basis. So in a way in the real world there are less criminals that you are likely to come into contact with. On the Internet, you just know you are going to be more vulnerable."*

> *"I think you have to look at the statistics, I think that shows that there is more Internet fraud than anything else."*

Whether or not statistics show that there is more Internet fraud, and whether or not this is due to increased and widespread usage of web-based transactions and/or a combination of other issues, the advantages and convenience of ICT mediated services prove to be an important mitigating factor:

> *"The reason I go on the Internet is because I'm physically removed by miles, like a three hour drive from shops, so yes, I appreciate the Internet in order to buy books and clothes that I can't get near me."*

> *"I buy a lot of things on line because the price is cheaper."*

> *"I don't have time to go out to the shops, I do my shopping on line. I can't be doing with sitting down and writing letters and then going off to the post office and getting a stamp and putting it in the post box, I communicate with my family by email. I wouldn't be able to run my little business if it weren't for the fact that I can do everything that I need to do over the Internet. The benefits outweigh the problems, it's making life more manageable for me, and massively more convenient and it means I have more time to spend with my family which is the key thing."*

Many felt that the risks are about equal and again, the advantages of ICT mediated activities are shown to have an important role:

> *"I say the outside world is just as risky."*

> *"I'd say about equal, I know that these issues exist and maybe I should be more concerned about them than I am. The practicality of it is that doing things electronically means that I can live my life in a way that I can do so many different things that I just wouldn't be able to do if I had to do everything in person, or go to so many different places."*

In this part of the discussion process several attendees related experiences where they had been the victim of cyber crime, for example:

> *"People do steal your details and I've had my details stolen a couple of times and my credit card details used, you know, online shopping fraud, and that's a real risk and it happens frequently."*

It is interesting to note that some expressed the view that it is possibly easier to manage risk and protect against becoming the victim of crime in the physical world and many felt more confident of managing risk in this environment than in the digital world:

> *"In the physical world if there's a risk you can move yourself away from it, you might not walk home down a dark alley on your own with a thousand pounds in your back pocket. On line, you don't know what the risks are, you're not so aware of them."*

> *"In the physical world it's easier to recognise the risk and avoid it, it's more manageable. In the online world management is more difficult. I feel better equipped to manage the risk in the physical world."*

> *"In terms of what I'm more likely to be a victim of, I'm sure it's online because there's far more scope for it and I don't frequent some of the places where crime rates are higher."*

However many attendees maintained that the same protection that exists in the physical world can be accomplished in the cyber world, albeit with a different model of risk management.

> *"You have a more manageable risk in the physical world than you do in the electronic world. You're more in control, if you want to take risks you can, I felt better able to manage the risks in the physical world because I've got built in threat detection, instinct. I can do things to manage the risk in the electronic world too but they are just different things and I need a different kind of threat detection."*

Some attendees said they felt less at risk of cyber crime than of being the victim of a crime in the physical world. The main reason for this was due to a sense of safety in numbers; attendees expressed a belief that there is so much electronic data held on so many people worldwide that statistically speaking the chances of being singled out as a potential victim of cyber crime is tiny compared to the risks in the physical world:

> *"I'm more at risk in the physical world, definitely. Why would anyone want to hack into my system?"*
>
> *"The statistical chance of you being hit is astronomically remote in comparison to your chances of say a burglary."*
>
> *"There's so much information floating around, the risk of someone hooking into you is so low level."*

This attitude is constructed from the misinformed belief that an attacker will only be interested in a system in order to obtain data from it. There was an apparent lack of awareness about the problem of botnets[26], which never emerged in any of the focus group discussions. This suggests that participants were not aware that a system may be a valuable target in order to steal resources (e.g. processing, storage and network connectivity) as well as data.

Relying on a statistically small chance of becoming the victim of cyber crime may be considered to be somewhat naïve but it is a relatively widely held opinion across all groups. A common theme running through all the workshop discussions is that we have to accept risk, for example:

> *"It's nice to have fun on the Internet, and to buy things but there are so many things that can go wrong. But then life's risky."*
>
> *"I think well, I've done it anyway and it's risky but you can't not do things because it's risky."*

Because cyber crime is difficult to detect and trace some attendees felt that it was unlikely to be resolved. Some voiced the opinion that police forces are under-resourced to deal with such activity and are unlikely to be able to bring the perpetrators to justice:

> *"If you send the police force an e-mail to say 'I've just been defrauded by an Internet fraud, they will quietly delete that e-mail, they will not act on it and the reason they will delete it is because it's impossible for them to solve but if they record it, it's a crime. So what happens to them is they have to measure crime, which is how many crimes they solve against how many crimes that are reported, so the figures would get worse."*
>
> *"The message that I get is that no action is taken against the perpetrators of these things because there is no power to do so. So I think there is a feeling of vulnerability to crime on the net because the people who are trying to perpetrate the crime are themselves not accessible to law enforcement or to action against them."*
>
> *"The government should be responding to changes in crime patterns and to ensure for example the police force have the sufficient funding for the number of forensic computer crime squads around the country as they do in other areas of forensic police work. I am not sure whether the government have actually responded in that way but if they haven't then I suggest that they should."*

Some attendees suggested that major Internet fraud is suppressed by business in the interests of maintaining a perceived level of security and trust in order to engender continued confident use:

---

[26] Canavan, J. 2005. *The Evolution of Malicious IRC Bots*. White Paper, Symantec Security Response. http://securityresponse.symantec.com/avcenter/reference/the.evolution.of.malicious.irc.bots.pdf

> *"I cynically believe that major failures of security in the net in terms of information getting wrongly revealed or accessed fraudulently are actually suppressed. The damage limitation is quite rife in major business, it has to be."*

How these and other factors impact on e-commerce relationships is developed in the following section. It should be noted here that just as opinions have changed regarding the likelihood of ID theft (see section 4.1) opinions as to the risk of being the victim of cyber crime are also likely to change with time and increased levels of use and exposure to ICT in a variety of contexts. A recent survey[27] by Get Safe Online Week[28] suggests that 21% of people now believe that they are at risk from online crime, up from 17% last year. As we see changes in detection levels of physical crime with increased use of DNA profiling and surveillance techniques it is quite possible that cyber crime will become a more attractive prospect to the criminally minded, where the risk of detection is lower.

3.2 Risk and Responsibility in E-Commerce

As we have described, attendees were sceptical about the security of online services and were aware that risk is involved. It is not simply a case of trust versus risk however, obviously there is a far more complex relationship here between user perceived risks and user perceived gains in ICT mediated transactions. We asked attendees about why they trust or do not trust a particular web site in the context of e-commerce and almost all were familiar with looking for signifiers of trustworthiness and were aware of the need to be protected:

> *"If you look for web sites with that special lock, when you are paying for things, when you see that you know the site is safe."*

> *"You might look for one of those badges that says 'verisafe' or whatever. They're not necessarily always something that you can rely on but it's a good indicator."*

> *"Do people know that when you connect to a secure site, you see the little padlock at the bottom of the screen? That's saying it's a secure site, and that's an international symbol."*

The comments above suggest that some attendees used security logos simply as a picture that signified reassurance rather than something they could click on to check security levels. Signifiers of site trustworthiness are necessary of course but many attendees were highly aware that they are not sufficient. Signifiers of trustworthiness can be copied or misused, hence this impacts on their effectiveness and reliability:

> *"At the end of the day it's just a little icon on the screen and I'm sure that can be copied, the same with logos or anything else."*

> *"I find with the certificates they're really quite often not used properly, the number of times for example that I've had a box coming up saying this organisation hasn't yet registered its certificate, which to a large extent defeats the object of having a certificate in the first place."*

> *"If there is a padlock in the corner, I trust this more now because there's a padlock there but it says nothing as to the reliability or security of the site."*

> *"You should theoretically get in the bottom right hand corner a small box marked SSL I believe, and if you click on that it will show you are on a secure site. Unfortunately some fly by night firms have found you can forge that easily.*

[27] http://observer.guardian.co.uk/uk_news/story/0,,1890363,00.html

[28] getsafeonline.org

So basically you click on it and up comes the certificate and it doesn't mean a thing. There is no answer to it, if you are going to be a victim of credit card fraud, it will happen. There's nothing you can do about it."

Obviously positive past experience of use and negative trust experiences influence e-commerce activity but we also found that buying decisions were commonly based around trusted companies that attendees had previous experience of using in the physical world, either by mail order or in face-to-face transactions, but reputation also played a highly significant role and tended to be centred on brand and prior experience:

"It doesn't matter if you're HP, BT or anyone else, the thing is to try and give people something they can trust, obviously you've got brand and whatever to rely on and things like that."

"Brands like HP generate trust."

"I was buying a TV and it was £500 and there were some cheaper sites and there was like £20 in it but I decided to go for a name that I recognised which was Comet, rather than one of the dodgier sites like these ones that bring everything over from France."

Brand and reputation go hand in hand and clearly impact on buying decisions even when goods can be purchased at reduced cost from lesser-known commercial organisations. However, negative impact on brand and reputation can occur when one person in another's trusted social network has a negative experience and this 'knock-on' effect can occur much faster in the digital world than in the physical world.

We also found cases where attendees actively sought opportunities for reassurance if they were considering a web-based transaction with a supplier they knew little about:

"I do buy from people I don't know but what I do is if I can find some contact details, I'll phone up to chat about the product."

This suggests that provision of alternative means of contact, especially a telephone number, enhances the likelihood of building a trust relationship because it provides the opportunity for a more richly cued environment than is available via web-based transactions alone.

3.3 Factors that impact on risk taking

In looking at building and monitoring trust relations we found that recommendations from trusted sources within an individual's social network play a major role. We found a great deal of evidence of what we might term 'second-hand' trust where workshop attendees relied on the positive (and negative) experiences of friends and relatives using particular web sites and ICT mediated services in the decision making and risk evaluation process:

"Past experiences, you've got the high street chains. Then friends, etc. recommend a site that they've used, and things like that, it's an association. If no one has heard of it, I won't use it."

"It's like a network of trusts isn't it, if somebody else trusts this person and you trust them, then you're going to trust this third party. Then you build up this huge network where everyone trusts everyone else, but it only takes one person whose trust is abused for that to go back through the network and then you don't trust that person or that third party any more."

"My Mum just phones me up, I'm her trusted resource."

Attendees cited several examples where a chain of trust is required after an e-commerce transaction has taken place and mentioned several ways in which this could be broken, for example:

> *"I might trust Amazon but I don't necessarily trust the post office who have the responsibility for sending on the goods. I may choose to pay with an online payment authority and that's another link in the chain that is also vulnerable so it's a risk. There are different risks at various stages."*

A commonly used technique to reduce the potential effects of credit card fraud was to have a credit card dedicated to Internet use or to use a different account:

> *"I change my credit cards, I've got one that I use specifically for the Internet, it makes me feel more secure that way."*

> *"If I buy something on the Internet then I use the account that hasn't got much in it, that reduces the risk."*

> *"You need two accounts really, one for Internet use and one that you would never ever give your details out on the web that has most of your money in it. I do that."*

> *"If I am going to spend £121, in my account is £121. Now, if someone hacks in and gets my details, they won't be able to get anything because that's all that's in there, and my bank is instructed not to honour anything above £121. And if they do, it's their loss, not mine. Now, you can't do it if you are buying ten things a day, but I've bought a couple of things online in the last couple of months from my "number 2 account." It sounds ever so clever but its not. I perhaps keep £25/£30 in that account and when I'm going to buy something, the day I buy it I call the bank and transfer the money into the account."*

Attendees were fully aware that credit card fraud and identity theft issues are not specifically related to e-commerce activity and could equally occur in the physical world:

> *"There are always ways and means whether it's by phone or mail, or handing your card over or whatever, it can be misused."*

> *"People can go through your rubbish and get all your details that way."*

> *"It's not just a case of taking your card away in restaurants or whatever, they don't even have to take it away from you. They can attach the software to the card reader and it can be there in front of you and you won't necessarily notice it unless you know what you're looking for."*

> *"If I pay in a shop or restaurant with a credit card, I never let it out of my sight. It never goes round the back. I'll say I'll pay at the counter, and I'll go up with them."*

Nonetheless, many attendees were of the opinion that there was greater opportunity for fraud to occur in the electronic world, less ability to trace how it had happened, and less likelihood of the perpetrator/s being apprehended.

3.4 Mitigated risk

A few attendees were very cautious about commercial transactions over the Internet and would only buy from sites they knew and trusted:

> *"I'll use a credit card but I'm very particular about the sites I buy from. If I don't know who the company is, I won't use them. I put my own security in place, if I don't know who the company is I won't give them my details."*

However, of particular significance is the fact that attendees cited many examples of e-commerce activity where they felt they had taken a risk by buying from a web site they did not know or consider to be trustworthy, or even explicitly didn't trust at all:

> *"I've used web sites that look very dodgy, that I've never heard of and nobody else has ever heard of."*

> *"I don't trust this site, they're a bit cheaper than say Amazon, I've never heard of them before but I still used them."*

The reasoning behind the use of such sites is revealed in the fact that hand in hand with risk goes responsibility; in every case of using potentially untrustworthy sites attendees cited the fact that their credit card company would foot the bill if something went wrong:

> *"If I'm buying something on line with a credit card in the back of my mind, even if I don't trust the site, is that my credit card is protected against that, they say in their blurb that if there is an unfortunate incident like that then they will pay."*

> *"I'm not worried about giving out my card details, I've got mitigation insurance, if a card gets cloned, kill the account, it's the bank's problem."*

This finding implies that where a third party, e.g. a bank or credit card company, can make restitution, attendees feel far more confident in making transactions with suppliers they feel may be potentially untrustworthy. In fact, from the users' perspective it could be argued that the risk is considerably diminished, mitigated almost to the point where it becomes negligible as responsibility for any negative outcome is shifted to a third party. Similarly it could be argued that such transactions do not require trust in the supplier to meet expectations, rather they require faith in the bank or credit card company to cover the loss. Where this is absent, or where restitution cannot be made or negative outcomes cannot easily be dealt with or mitigated the scenario is quite different, hence responsibility for restitution of loss is a significant factor in e-commerce relationships:

> *"I work in banking and some banks say that unless you can prove otherwise it's your fault, you gave out your credit card details, so you do have to be careful, you are responsible to use it correctly."*

> *"The law is actually quite clear, in the UK anyway, there may be problems elsewhere but in the UK, the banks may try it on but if you take out insurance it's their problem not yours."*

Some attendees felt that the banks were not taking enough responsibility for introducing technology that could improve security:

> *"I think the banks are liable, I think they're liable in law. I think the problem is that from a cost- benefit analysis perspective, which is what they're using, it costs less to give you your money back and write it off than it does to prosecute and do something about it. So from their perspective the investment to fix the problem is greater than just quietly making you go away and giving you your money back."*

> *"I don't trust the banks one jot. Their approach to putting in technical controls that would help protect you against fraud and other scams is farcical, they're being much too slow, they're not utilising technology that's available to date to solve today's problems and their plan is to act in five years rather than next year."*

This suggests a certain degree of distrust in banks and financial institutions more generally, however none of the attendees complained that their bank had failed to make redress in cases where they had been the victim of fraud.

3.5 Irrelevant and excessive data collection

Privacy and control of information given up in e-commerce transactions was also of concern to attendees and many gave examples where additional information was required that they did not feel was relevant to the transaction and/or was excessive:

> *"Even when you go on Amazon, it wants to know all this stuff and then you go and register somewhere else and it wants your email and your phone numbers and all this, so you actually end up giving out a lot more data than you would if you just went into a shop and bought something off a shelf."*

> *"It comes back to privacy, mind your own business, what do you need to know that for?"*

> *"I don't know what the future's going to hold, and I think you have to realise what the implications are. I was just thinking what sites I don't buy from – its American companies who offer a free product but still ask for all your details. I don't do that."*

Attendees also gave many examples of giving false information wherever possible if they did not deem it necessary to the transaction and this highlights the fact that much electronically held data is inaccurate:

> *"I think people don't want it to be accurate, that's the thing, nobody wants them to hold that data, that's why we make it up."*

> *"I put in rubbish data if I can't bypass it. Unless there's a reason for them to know my address, why should they have it?"*

In some cases where information was required that was perceived as excessive and irrelevant attendees reported aborting the transaction:

> *"It's the fact that you're asking people to sign, in my opinion, an unconscionable contract that is at the heart of this, that's not how you build trust."*

> *"Unless I desperately wanted to use that site I'd go somewhere else."*

> *"If it's in a required field that can put you off."*

Our research suggests that there are three important elements that help to make people feel more secure in e-commerce transactions: confidence that restitution can be made by a third party, assurances about what can and cannot be guaranteed, and the presence of fallback procedures if something goes wrong as shown in the quote below:

> *"Given that it's actually impossible to make a secure system, perhaps banks and all the rest of them should stop telling us that it is secure, and rather, they should be taking measures to try and make it as secure as possible but assume that sooner or later it will be hacked, it will be broken into and with that assumption in mind, then what are the procedures?"*

Our discussions in this area have revealed a relationship between trust, risk, privacy and control of information, responsibility, and levels of confidence in relation to the likelihood of restitution being made if loss is incurred. Clearly this is a complicated equation that is likely to comprise even more elements than those identified here. For example we will further explore traders' expectations in e-commerce, and indeed, whether they know what those expectations should be, as well as the impact of certainty and uncertainty on whether those expectations will be met. In terms of risk, responsibility and restitution we will further explore what is at stake for the individual as it is clear that just as different assets have different values to different people in the physical world, this is also likely to be true in the field of e-commerce and the digital world more generally. The comment below from an attendee talking about a car hire experience illustrates this point:

> *"It was a three day hire…if it was the first time I'd used them and something went wrong I wouldn't have used them again but it wasn't the first time. And I was on holiday; if it had been for work and I'd missed an important meeting I probably wouldn't use them again. But I got the car in the end and they were*

> *very apologetic and they extended the hire period because they realised they'd made a mistake. But if it had been the first time I wouldn't have gone back."*

Responsibility for the consequences of negative trust experiences also deserves further research since the seriousness and/or impact of the consequences is highly variable.

4 Authentication and Identification Technologies

Authentication and identification processes inherent in ICT mediated activity are commonplace, most of us are now familiar with the requirement to prove who we are to a given system whether that is via a password or PIN number or a combination of methods and this can add to a sense of security, for example:

> *"I had a problem with Paypal once because they thought someone had changed the details on my account and I thought that was quite reassuring. I then had to go into Paypal and they ask you certain security questions and those sorts of things, I'm fairly confident if there's four or five questions personal to me."*

Not surprisingly we found high levels of awareness and use of current identification and authentication technologies and both of these aspects are considered in the following sections.

All attendees stated that they had some level of personal experience of card-based payment systems, especially those that accept credit cards like MasterCard and Visa. As discussed earlier, when using these cards often the question of trust in the organisation receiving the payment was overlooked because any risk of fraud was considered to be mitigated by the card issuer, typically the bank. Even when the question of possible fraudulent signatures was introduced, attendees continued to consider any fraud to be "not my problem."

4.1 Chip and PIN

Swiping cards and signing for purchases has become normal practice for purchasing activity but vulnerabilities in this process have increasingly been exploited by criminals with predictions that annual losses would rise to £800 million by 2005 if changes were not introduced to combat fraud[29]. Such changes were introduced with chip and PIN cards in 2004 and this became mandatory for use in shops from February 2006. In effect this change mounted a two-pronged attack against fraud by upgrading the technology on the card itself as well as changing the means by which the card-holder is authenticated at the point-of-sale[30]. Attendees were familiar with flaws in using a signature to authenticate a transaction (for example shop assistants not bothering to compare signatures) and some saw the introduction of chip & PIN as more secure:

> *"I've always thought it was a lot more secure than a signature because most of the time cashiers don't even look at signatures. It's so easy to forge a signature."*

For others the introduction of chip & PIN as a means to authenticate the identity of the cardholder made little change, and they felt that chip & PIN was no more secure than the system it replaces:

> *"It's not more secure, of course it isn't, it's easier but that's all."*

> *"I've been standing behind someone in Tescos and he was asked to sign because the PIN wouldn't work. And he said 'I can't, its not my card. I'll have to come to the cash point and get the cash.' He had someone else's card, perfectly legitimately, but it shows how easy it is to know your PIN and use your card. So I don't think it's any more secure."*

[29] BBC 2006. "Chip-and pin cuts fraud by 13%," BBC News Online, 6 March 2006. http://news.bbc.co.uk/1/hi/business/4779314.stm

[30] Steven Furnell, April 2005. "Safety in numbers? Early experiences in the age of chip and Pin

Attendees noted for example that it is relatively easy for someone to look over your shoulder and see the PIN being entered:

> *"Chip and PIN is a great step forward but it's also partially a step back. Once someone has got your PIN, you are completely exposed, and people on the other side of the till aren't checking [signatures] any more."*

> *"The PIN machine is wide open for anybody to look at. If I was into that type of thing, I could pick-pocket them on the way out and I've already seen their PIN."*

Some attendees felt that chip and PIN made them more vulnerable to fraud:

> *"I got my card cloned purely from chip and PIN."*

> *"Mine happened last month I got my debit card cloned, I prefer online shopping to chip and PIN."*

> *"Chip and PIN, basically you can use carbon paper behind that, as soon as you press your buttons there's a carbon paper behind the buttons that you press and then they can just take out what you've swiped and put in your details, they could look at your card, see that 3 digit number on the back which a lot of people now ask for, and they've got everything."*

For some chip & PIN offered greater convenience because it made the payment process faster and easier, a benefit promoted under the chip and PIN initiative[31]. Few attendees had recognised that with chip & PIN comes a change in the liability model, with merchants no longer being liable for card fraud where the PIN is used, i.e. they would only be liable if they allowed the customer to pay without using the PIN:

> *"It's shifting responsibility to me rather than the retailer, if there's fraud on your credit card in a chip and PIN situation it's you that carries the responsibility."*

Similarly, all but a few attendees had not realised that whereas a signature could in theory be disputed by the user, it would be far more difficult for the user to dispute a payment in which their PIN had been fraudulently used, thus potentially changing the model from 'innocent until proven guilty' to 'guilty until proven innocent':

> *"If someone has used your card illegally, then you probably can't get out of it."*

> ***"**When you use your PIN that is now you, whereas the signature in the past, that wasn't you, you could just say that is somebody else's signature, so I'm not sure what the law is yet with the chip and PIN but I think that's what they're trying to do, trying to enforce the use of cards in that way."*

Those who had recognised these changes were concerned, but reluctantly chose to continue to use the chip & PIN because of the convenience and on-going belief that the banks will underwrite losses.

These are issues that academics have highlighted as part of the on-going debate on the introduction of chip & PIN[32]. The concern surrounds both the use model and how responsibility for fraudulent transaction is attributed, and the reliability of the underlying technology, e.g. the smart card. It is clear that chip & PIN has changed the liability model, but not that this change necessarily affects the user, and that it could be more difficult to dispute a transaction that is authenticated with a PIN than one by a hand written signature. And, as several attendees commented, a PIN, if properly protected and used sensibly, is more secure than a signature.

[31] http://www.chipandpin.co.uk/consumer/index.html

[32] University of Cambridge http://www.chipandspin.co.uk

The effectiveness of the smart card technology was treated by attendees much as any other technology introduced to enhance security. Few attendees believed that the system could not be 'broken', and accepted that in time, if not already the case[33], cards will be defeated, citing the recent case where Shell suspended card use at their fuel stations.[34] (Note: The attendee below mistakenly cites BP rather than Shell):

> *"All BP garages have suspended paying through credit cards because someone has hacked in and got all the credit card details of their customers."*

For some attendees the PIN was considered to be less secure than a traditional handwritten signature and an inconvenience because it was something else the individual had to remember:

> *"Chip and PIN isn't secure either, it's safer to sign for something."*

The usual strategy of setting the PIN for all cards to the same value, discouraged by the banks but clearly something attendees do, was also recognised as a potential weakness that could be exploited by an attacker:

> *"I still need to remember my PIN; I use the same PIN for everything."*

In fact, some felt that the security of chip & PIN was that a physical card had to be present every time a purchase was made, and that as a consequence they should take particular care not to lose the card:

> *"Chip and PIN is only safe so long as you don't lose your card."*

The introduction of chip and PIN has done little to change attendees' perception of trust in the technology or systems that enable card payments, mainly because they believe that they are protected from fraud by the banks. Attendees do not currently feel the need to trust the technology and seem likely to remain sceptical about any claims of increased security. Having said that, chip & PIN is seen as a low risk, convenient and easy to use payment method.

4.2 ID cards: An aid to security?

The subject of ID cards was introduced in the workshops as an aid to security and a means of easily identifying or authenticating oneself. It is interesting to note however that the discussions developed around the theme of increased vulnerability rather than security, for example:

> *"I feel more vulnerable having all my data like personal details held in one place electronically than I would having ten separate paper documents held in different places."*

> *"Everything I've read on ID cards shows that they are just crossing their fingers; they actually believe that it will be secure and I don't believe that, not at all."*

> *"If you can guarantee that the government can keep that information completely safe and completely secure from those people that don't actually need to use it, I think they're fantastic but I'm sorry, I don't think they can."*

---

[33] Attacks where cards are forced to 'fall back' to their magnetic stripe have been reported in The Guardian (May 12, 2006): Chip and pin pushes card fraud abroad, http://money.guardian.co.uk/scamsandfraud/story/0,,1773447,00.html

[34] From BBC News (6 May 2006), "Petrol firm suspends chip-and-pin", http://news.bbc.co.uk/1/hi/england/4980190.stm

It is interesting to note that some attendees interpreted the potential introduction of ID cards as evidence of Government's lack of trust in its citizens and felt that this would be detrimental and change the relationship irrevocably:

> *"One of the fundamental problems with ID cards to me is they change the relationship between the citizen and the government of the country."*

> *"If ID cards are brought in it's now officially legitimate for the government to know who I am and where I am all the time, no matter where that is and it's officially legitimate. We can no longer complain about CCTV cameras and car registrations and GPS cell phones because we've passed legislation saying the government has a right to know who I am and where I am any time they want."*

It is not surprising that the subject of restitution and guarantees also arose in context of identification and ID cards, whereas restitution can be made relatively easily for financial loss, the same cannot be said of losing one's identity:

> *"If someone hacks in and changes part of the data, then it could identify a different person as being me."*

> *"I think the guarantee that makes the ID card worth the paper it's written on is unachievable."*

Allied to the point above, the discussion also highlighted the way in which risks can impact on trust and confidence. Although the comment below was made in the context of identity theft it clearly highlights the need to look at the impacts of failure and the need to mitigate any these with effective fallback mechanisms, and this holds true across all ICT mediated activity:

> *"Assume identity theft is possible, what are the procedures to work it out again and get it all sorted? If people knew what would happen if their identity was stolen through one of these identity cards, if we knew how to get out of that situation then maybe we would trust it more because we know what the risks are. At the moment we've no idea what the risks are so everyone is getting nervous."*

> *"At some point there will be clones of these so what are we going to do then, and what's the next rabbit that the government is going to pull out of the hat? Is it going to be even more repressive measures for ID, is it just going to be a technology change, god forbid that would cost another 'x' billion pounds to roll out?"*

> *"Security will always be breached whatever kind of security you introduce. You've got to assume it will be breached by someone at some time."*

The high degree of distrust of ICT services and applications more generally was surpassed only by an intense distrust of electronic data gathering, storing, and the potential for misuse. The quantities of electronic data held about individuals and the purposes to which that might be put now or in the future were of most concern, especially where it involved storing ID information on a central database:

> *"We've got so much information held about us that is stored electronically, reams and reams more stored than we ever would have in the paper world so it's not just about whether you've either got this information in digital form or on paper, there's a huge discrepancy between the amounts of information and the different places where it's stored."*

> *"I get worried by the idea of having a single identity card, it's a lot harder to copy lots of different things like your passport, and a driver's licence for example, that's only two things I know, but if you have only one card then that's only one thing to copy."*

> *"Can I just say that I was working with friends in America and they went to the library, and post 9/11 the government were allowed to access library records. And people were taken into prison overnight or longer because they were seen to be potentially causing civil unrest. And that's just from library records and saying it's for your protection. Some of them were very innocent, just environmental activists."*

Strong feelings were voiced about the security of information held on individuals and new possibilities for fraud that would arise if data fell into the wrong hands. Attendees also voiced strong concerns about the potential for a black market in counterfeit ID cards. Very few attendees thought that ID cards would aid either their personal or the nation's security and concerns were mainly centred on Government's ability to hold ID data securely because of the high appeal of such information to hackers:

> *"I don't think the government are very good at IT and it's bound to get hacked."*

> *"It won't make us more secure, that's rubbish, it's a hacker's dream, terrorists will be the first people to hack into it."*

> *"If the government isn't going to be open about what they're doing then that means the security must be poor because nobody is checking it, nobody is pointing out the mistakes they're making, so somebody will find a way in. There may be all these secret plans for what will happen if it goes wrong but surely they should be open about it, if we're supposed to trust them."*

It is interesting to note that it is not the carrying of an ID card per se that attendees object to but rather the increased sense of vulnerability resulting from having such data about them held electronically and the possibility that this could be stolen as evidenced in the statements below:

> *"It's not so much the card that's the problem as the database, the fact that the government are putting all the data they have about me in one place creates vulnerability. It's nothing to do with the card itself."*

> *"The problem is when you get all the information in one place, and that is your identity. That's the problem with the identity card. If somebody has that card with their face and your biometrics or whatever, they are you because that card says so."*

> *"I don't have a problem with photo ID, my problem is there are going to be certain people who can clone your ID card."*

Some workshop attendees had experience of holding an ID card in other countries and could see the value of the card as a means of identifying themselves where none other was available:

> *"I've lived abroad where we had to have an ID card, I can slip it in my wallet instead of carrying my passport around with me for example, and when I need to go into buildings and I have to show ID I can use that. I don't drive, I don't have a driver's licence so I can't use that as a form of ID."*

However, approximately half of workshop attendees said they would not voluntarily carry an ID card. Concerns about the requirement to hold a card and infringement of civil liberties are high on the agenda for many and it is difficult to see how these objections can be overcome if registration is made compulsory. Attendees also objected strongly to being charged to obtain a card, and were concerned that once introduced, legislation would be changed to make carrying the card compulsory as has occurred in other countries:

> *"They brought in legislation that said you said you had to carry this card on you at all times and you can be fined if you're stopped by the authorities and you haven't got it with you, that's when I've got a problem with it."*

> *"Why should I allow the State to hold information about me? To what purpose? Who's in charge of my life, me or the State?"*

Allied to the point above, there were also concerns about the lack of control in how the data might be used initially and how that use might be changed in the future due to the potential for 'function creep':

> *"You don't know what you don't know, you don't know how the data might be used."*

There was also little faith in ID cards achieving Government objectives:

> *"The fact that we have an ID card, it's not going to stop what it's purported to stop so the question is, what are they going to be used for? And because there is a difference between what they're being advertised as being used for, and what you think they could be used for, you're trusting the people who are requiring you to have them and when that trust fails then it becomes a problem."*

> *"The politicians have always said it's there to frustrate terrorism, not to stop it, it's there to help them the fight against crime, not to stop it. That's what they've always said, however, when it has been presented as something that 'will stop terrorism, it will stop crime', they themselves have not actually put their hands and said 'no actually we only said it would be an aid'."*

The highest levels of resistance to ID cards concerned the possible addition on the card of biometric data. Again it is interesting to note that this does not concern the carrying of a card per se:

> *"I just don't like the idea of the State having that kind of information."*

> *"I wouldn't carry the ID card with biometric data on it. That doesn't mean I wouldn't carry an ID card."*

Overall these findings are similar to those resulting from previous work in this area conducted by BT Research and Venturing[35]. Although attendees are not averse to carrying a card in principle and often described themselves as 'law abiding citizens, who have nothing to hide,' they are not convinced of any benefit to the individual. Government envisages a range of services that could be accessed via an ID card and it is important to stress the advantages of holding a card if it is to gain the required levels of public acceptance. The UK is increasingly a card-carrying society, e.g. Oyster cards, ATM cards, credit cards, debit cards and store cards, but fundamental to understanding how Government might achieve a broad level of acceptance of ID cards is the need to understand *why* we carry cards. All the examples noted above have tangible benefits to the carrier and an ID card will need to have similar advantages before it will be perceived as serving both individual and public interest.

4.3 Use of Biometric data

Biometric options for identification and authentication purposes are already being actively pursued, as for example in the case of iris recognition at airports and finger-print scan payment technologies[36]. Discussions about the use of biometric data raised similar issues to those concerning ID cards. We asked attendees about the use of biometric data as a more reliable means of identification and authentication than existing methods such as passwords,

[35] May 2003, Lacohee, H. Response to Parliament's Consultation Points on Entitlement Cards and Identity Fraud. BT Report undertaken as part of the 'Frightened Society Project.'

[36] Best, J. 2006. "Oxford Co-ops test finger-print payments," silicon.com, 8 March 2006. http://software.siliocon.com/security/0,39024655,39167057,00htm.

chip and PIN and security questions about personal information. There were high levels of scepticism and negativity around the use of biometrics and some biometric data was seen as far more controversial than other forms:

> *"There is no solution that's fool-proof, because they are all built on technological decisions. DNA for example, they've had several trials where DNA evidence has been ruled as inadmissible because it often gets corrupted. DNA, by its nature, is an evolving piece of paper. Iris recognition doesn't work either; irises change over time."*

> *"I was automatically suspicious with somebody asking for my photo identification, my thumb print or my eye, that sort of security I'm afraid, I find it an invasion of my privacy."*

As noted earlier, the highest levels of resistance to the use of biometric data concerned our discussions around the use of ID cards. Some felt that the storage of biometric data would actually make individuals more vulnerable rather than more secure. These concerns were centred on the need to hold biometric data in a database that would be vulnerable to attack. Many felt that on balance biometrics were no more secure that any other security scheme:

> *"You are assuming that these levels of technology are in some way adding some kind of safety, when in fact all they are doing is just creating more data that is equally as manipulable as your servers are."*

> *"All databases have inbuilt errors. My fingerprint might be infallible but the system behind it is not."*

> *"The more complicated the data you are holding, the more data you are holding, the more inter-relations between that data, the more margin of error, the greater the probability of error occurring."*

Because biometric data is deemed to be more accurate than other means of authentication the need to protect that data was seen by attendees as extremely important:

> *"The greater the trust you put in the infallibility of a method for identifying you, the greater the protection of that information needs to be."*

Allied to the point above, the impact of having biometric data stolen is considered to be far greater than the impact of identity theft via other means because biometric data is perceived as much more difficult to recover and restore:

> *"The end result of the identity theft would be that much greater."*

> *"If we did have this fingerprint ID or iris ID on our financial cards, not ID cards, what liability would the bank accept or suffer when there was a fraud and the hackers found a way round that and there were mistakes because the system is run by human beings? So there's always going to be mistakes and slip ups whatever, it's like what happens when the fingerprinting doesn't work, what happens when the iris doesn't work?"*

Similar concerns were centred on technical errors in the systems that read biometric data:

> *"So what happens when you go in to this thing, and it is you, you know, your fingerprint. You put your finger in the pay thing, but they have screwed up somewhere, because they've got a technical employee who accidentally deleted some file and replaced it with a part of something else. They say that's not you. How are you going to prove that's you, when their database says that's not you?"*

No single source of biometric data can be one hundred percent effective or cover one hundred per cent of the population and many attendees were concerned that biometric data is not accurate and were aware that readings can give false negatives and false positives:

"The accuracy is still very questionable."

"One of our customers uses fingerprinting but only about 80-90% of their customers can actually use it on a regular basis, the other 20% have to enter an ID number, just because that's the day it doesn't work and for some people it never works, for no apparent reason, it just doesn't. So I'm concerned that if biometrics became the only way of identifying yourself, there are days when it wouldn't work, and for some people it will never work, and then you've got the accuracy problems. It might make an error one in ten thousand times but if you're using it all the time, as in an airport, then that's going to happen every hour."

Our discussion around biometric data resulted in some fairly heated debate about why it is necessary to be identified with increasing levels of accuracy, by whom, and indeed, the need to be identified at all, in an increasing array of diverse situations. Much of the discussion focused on the opinion, held by many, that they can already identify themselves via a variety of means:

"Why do you need to prove who you are? What does it achieve?"

"If I'm travelling on a plane I know I need to go there with a passport so it's me, plus a passport."

"Why do we need to prove our identity so strongly?"

Most of our attendees were of the opinion that they could adequately identify themselves in all situations where they are required to do so and very few thought that additional identifiers were necessary. Of particular concern was how restitution could be made if such information was stolen or misused and the need for measures to be put in place in the case of faulty readings.

4.3.1 Fingerprints

Fingerprinting is considered by most attendees to be the least invasive and most acceptable form of biometric identification. Even though fingerprinting has the unfortunate connotation of criminality most were comfortable with using fingerprints for authentication. However, in practice there was evidence of objection that suggests that acceptance of this means of identification may be context specific.

The use of fingerprints in a national voting system was considered by some to be an acceptable means of identification but other attendees related experiencing the requirement to provide fingerprints on entry to airports in America and this was deemed far less acceptable, for example:

"I actually complained to the woman at the desk but there was a man with a big massive machine gun who told me that I had no choice whatsoever."

As noted above, the Co-operative Society have recently introduced fingerprint reading as a means of purchasing groceries that also replaces a customer loyalty card[37], and prior to this Pay by Touch schemes have been deployed in US stores[38]. When introduced to this idea some attendees thought it would be acceptable and would save time in queues while people pay via more traditional methods. Others envisaged a range of privacy related problems:

[37] http://news.bbc.co.uk/1/hi/england/oxfordshire/4784744.stm

[38] San Francisco, CA, July 22, 2004 - Wallets are out, and fingers are in. Now, there's a better way to pay for your groceries. http://www.paybytouch.com/news/pr_07-22-04.html

> *"I really don't want Tesco to have my fingerprint, just in case Joe Bloggs hacks Tesco for fun and finds my fingerprints, and then goes and hacks in to the criminal records database and finds out whether I have ever been arrested or not, and then uses that information against me."*

In fact Pay By Touch finger scanning technology does not store actual fingerprints; instead it creates a set of geometric points that allow for a secure identity match at point of sale but attendee perceptions again highlight the need for better education of how such technologies actually work. Some felt that fingerprinting could not be trusted to the extent that some organisations are claiming:

> *"I don't consider fingerprints to be secure any more. They take my photo when I go to the disco, they copy my iris."*

Most attendees expressed the opinion that fingerprints were a reliable means of identification probably because of their successful and well-reported use in crime detection. It is interesting to note that although the same is true of the use of DNA in this context, it is considered to be a far less acceptable means of 'common' (as opposed to criminal) identification as discussed in section 4.3.3 below.

4.3.2 Iris recognition

Iris recognition was considered to be more secure than a password (because, like fingerprints it is uniquely related to the person), but attendees still voiced concerns about this in terms of possible risks to health, for example:

> *"The first thing that crosses my mind when you say iris identification, is will that technology damage my iris or retina and on that I can't say 'oh yes, I trust that, I trust the use of that', I want to know if it's going to hurt me. What kind of assurances can you offer me that it won't hurt me?"*

> *"I've got eye damage so I would be reluctant to expose my eyes and would want to explore this before I'd do that."*

Attendees were also concerned about information being transferred to a database where it could be vulnerable to misuse. However, it was also viewed as a quick means of identification and that might impact on its acceptability:

> *"If you are just looking in to my eye as I am going through passport control, thank you, that's it. If somebody at passport control wants to swab my mouth that's different."*

Iris recognition was perceived as likely to give false positive and false negative readings and was not generally seen as completely reliable although some attendees thought it presented a more reliable means than current authentication processes:

> *"Iris recognition, you know these things are being sold as fool-proof methods but they're not."*

> *"I think of iris recognition as being better than what I have got at the present time."*

Again some attendees had experience of iris scanning at US airports (and a trial has been conducted at Heathrow[39]) but were unsure as to whether this was simply a photograph:

> *"It is an iris scan, is what they are doing, they say they are photographing your face, but they don't."*

[39] April 20th 2005 Heathrow to Hold Iris Scan Trial
http://news.airwise.com/story/view/1113955067.html

This highlights the need for straightforward and honest approaches to data collection more generally, and particularly in the use of biometric data. It seriously undermines public trust when biometric data is collected via covert means, or for spurious purposes. The most often cited example of this in the workshop discussions was the recently reported proposed Government plans to inflate police powers[40] so that they will be able to take the fingerprints and DNA of anyone they arrest, whether or not they are charged or found guilty of any crime. Such reports have led to (denied) claims that the Home Office is surreptitiously building a database of every citizen's DNA and most thought that this seriously impinges on civil liberties:

> *"The Attorney General for example, they've collected about seven million DNA samples, he was questioned about how they should be keeping this, and if people aren't guilty they should destroy that data and he says 'why would we want to destroy it?' They've got that data now, they wouldn't want to destroy it because people will be picked up because of those DNA samples. This information is collected and people who have it aren't going to throw it away, they're going to keep it and at some stage in the future it could potentially be used in a completely different way from that expected…"*

If such operations continue it is likely to provoke such a climate of distrust that it is unlikely that biometric data will win widespread public approval and acceptance as a means of identification in common, everyday situations or as a means of access to public services.

4.3.3 DNA

Attendees considered DNA to be the most sensitive and controversial piece of biometric information and most were unhappy with the idea of using this as a means of identification:

> *"Using DNA is massively different. I'm not comfortable with it."*

> *"The idea of central government holding a database of people's DNA is frightening. I think the very idea of giving any state that amount of control or even taking tentative steps towards doing that is so dangerous that it actually terrifies me."*

> *"I am happy providing biometric data, but not DNA."*

A minority of attendees maintained that they 'had done nothing wrong and had nothing to hide' and were therefore less concerned about any data that was held about them and were prepared to give up their DNA:

> *"I've got no intentions of doing anything wrong in my life, I'm not bothered about what people know about me, I'm not bothered about the government knowing anything about me, so I'm OK with it."*

A high degree of scepticism towards this view was expressed within most of the groups, for example:

> *"It's all very well saying well, I never intend to commit a criminal offence and if you've done nothing wrong you've got nothing to worry about, but that will change. At one point we had fairly liberal rules of process in this country but we haven't now."*

However, almost everyone viewed DNA as a highly accurate method of identification and authentication:

> *"If it's DNA then there will never be an error will there."*

[40] Police DNA powers 'to be extended' http://news.bbc.co.uk/1/hi/uk_politics/2890047.stm

Despite this high level of confidence in DNA as a means of identification it was considered by most as seriously vulnerable to database attack given the value of the information, and was considered very difficult to protect:

> *"Fingerprints and DNA – hair – is easily obtained because we leave traces of ourselves everywhere."*

> *"I think that is one of the problems with the whole thing about giving out your DNA, it's who else is going to have access to it and why, and the whole idea of the government having this data is very scary."*

Some expressed concerns that DNA profiling may be used to go beyond straightforward identity recognition or authentication and most of the issues raised concerned access to health information and the impact of that falling into the wrong hands:

> *"If you go into DNA though you're going down the insurance route, and that's even worse if they start profiling your health risks."*

> *"DNA is more worrying because health can be profiled."*

Attendees also voiced strong concerns in relation to 'function creep' and how biometric data might be used in the future:

> *"I would be in principle against it, I would be frightened about it, I would certainly be frightened about any, well say at a state of war, a government in a state of war would feel perfectly justified in doing all sorts of things with your DNA."*

> *"I wouldn't want to do it because I think for me personally its an invasion of my most fundamental human building block, it's who I am and what I am. There's nothing more specific to you as a human being as your DNA so I wouldn't want to do it because I would see it as an invasion of myself and also, secondly, I wouldn't want to do it because I wouldn't trust the authorities, the State, the banks whoever, I wouldn't trust what they would do with my DNA say in 10 or 15 years time."*

> *"How do we know that our DNA wouldn't be used to clone us perhaps in future generations? And also I think there's a lot of corruption in the police and the DNA could be used to affect a trial for example. If I'm on trial and they run my DNA through the system and find out that one of parents or grandparents was a serial killer, would I get a fair trial?"*

Many voiced concerns that biometric testing and DNA profiling would be imposed upon them in the future and this was perceived as unwelcome:

> *"It is inevitable that DNA will be used, we don't have a choice."*

> *"I think we are going to be forced to."*

> *"Once the technology is powerful enough, and there's no reason to doubt this, DNA will be scanned at birth. Security of a central database will be impossible. The receptionist in the local doctor's surgery will have access to the nation's DNA."*

Attendees argued that there is already evidence of Government imposing unwelcome restrictions upon them. For example Government claims that ID cards would be introduced voluntarily have been undermined by the proposed introduction of imposing cards on those who wish to renew their passports; the voluntary element of course is that people could choose to not hold or renew their passports:

> *"It's like the identity card or the passport thing, you can't renew your passport without having an ID card now."*

Obviously this is an unacceptable option for current passport holders and heavily implies covert introduction of compulsory ID cards. Such actions increase public distrust of the need for ID cards at all, diminish any perceived personal (as opposed to government) benefit and increase scepticism about future developments and plans for the card to carry increasing levels of data, despite government statements to the contrary.

5 Identity management, theft, privacy and fraud

Rapidly developing technology has enabled increasing volumes of data to be harvested and stored. Much of this information is necessary to the smooth and efficient flow of information, communication and delivery of goods, services and administration of government functions that modern society demands. However these rapid technological changes also threaten our privacy and security and we are ill equipped to deal with the consequences. Unlike financial loss, redress is far more difficult to achieve when personal information and identity factors are at risk and the repercussions can be far more serious in their impact on our daily lives. The sheer volume of electronically harvested and stored data, ease of access and poor security all contribute to a growing sense of vulnerability and lack of control over how our personal information might be used.

5.1 Identity theft

Identity theft is reportedly one of the fasting growing crimes in the UK, it is estimated that one in four people have had their identity stolen or know someone who has fallen victim to identity fraud[41]. Identity theft is a growing problem borne of our increasing dependency and use of personal information that affords new opportunities for crime not only in ICT mediated activity, but also in society in general. Awareness of identity theft and the likelihood of becoming a victim have increased dramatically; research undertaken by BT[42] in 2003 found that identity theft did not rate highly in the minds of the public even though at the time it was costing the economy approximately £1.3 billion a year. In 2003 we found that people rated burglary, car theft and mugging as the top three crimes that they were likely to fall foul of but our current research shows that attendees considered identity theft to be high on the agenda and this is supported by a recent survey by Get Safe Online that shows that people fear they are more likely to become victims of online crime than they are to be mugged or burgled.[43] The comments below illustrate this point:

> *"It's going to happen eventually, you get the impression that the level of this kind of activity is fairly and high and if you get through your life without having anything like this happening to you then I think you're probably quite lucky."*
>
> *"Most of the attacks are done on banks, or hijacking personal identities."*
>
> *"You can try and reduce the possibility by shredding stuff and things but I can't see how you can actually be proofed against it."*

A recent Home Office study[44] claims that ID fraud now costs Britain £1.7 billion and although there is some suggestion that these figures have been inflated and losses overstated[45], attendees clearly considered themselves to be more at risk of ID theft today than shown in the study in 2003. There is no doubt in attendees' minds that the amount of electronic data that might be stored about them increases vulnerability and this vulnerability is due in part to the blurring of the public and private domain. The prevalent belief amongst attendees that no data that is stored electronically can ever be secure leads to the commonly

[41] BBC News, March 3, 2005 http://news.bbc.co.uk/1/hi/business/4311693.stm

[42] May 2003, Lacohee, H. Response to Parliament's Consultation Points on Entitlement Cards and Identity Fraud. BT Report undertaken as part of the 'Frightened Society Project.'

[43] http://observer.guardian.co.uk/uk_news/story/0,,1890363,00.html

[44] Home Office: 2nd February 2006 http://www.gnn.gov.uk/

[45] Silicon.com February 2006 Public Sector News http://www.silicon.com/

held opinion that all electronically held data should be considered to be in the public domain because it is vulnerable to attack:

> *"The question is what's in the public domain and what isn't. If it's electronically held data then you might as well say it's in the public domain because somebody somewhere can get access to it."*

> *"If the data is there it's going to be abused by somebody."*

> *"With electronic data the problem is that it's so easy to access, you can just pull up a document. With paper documents, well, you're welcome to try and find out but you'd have to go through 15 thousand pages."*

There was a high degree of awareness of attempts at identity theft via phishing and several attendees were able to give examples of personal experience of this, for example:

> *"I just received a letter the other day to say that someone was trying to steal my identity, but now I'm wondering whether the letter itself was a scam."*

The dangers and implications of identity fraud are so high on the agenda for some that this impacts on use:

> *"I think it's very likely it's going to happen, my wife has never bought over the web because of that."*

> *"I only use services where I don't need to authenticate myself or identify myself in any way."*

> *"You buy something from Dell online, at one point you have to click a button to say you give up all your data protection rights because they are going to pump all the data over to America. So, now I can have whatever system I wanted up there, it could give me the same user experience, but then at some point it might say 'oh, because I actually want to buy this I have to give up all these rights, in the pump to America' no matter what systems are in place, you've just lost the trust of the users. So no matter what technology you put there, you don't get the trust of the users by changing the business practises, it's lost."*

However, one point of particular significance in the case of misuse of electronically held data is that we rarely know that it has occurred until the damage has been done, and it is very difficult to trace:

> *"I don't know what's happening to my bank details, who is trying to hack into that."*

> *"My wife's bought stuff over the net but she's been the victim of identification theft and the problem is that you can't track where that originated from. It may have originated from Amazon for example so you don't know who you can trust."*

For many it is this unknown element that engenders the most concern and is most likely to adversely affect acceptance and adoption.

5.2 Collection and Use of Personal Data

The collection and use of personal data pose new dangers to privacy[46] and attendees were very aware that increased data collection and storage made them more vulnerable to identity theft, particularly when information is held in centralised data bases:

[46] Solove, D. J. 2003 Identity Theft, Privacy, and the Architecture of Vulnerability. Hastings Law Journal, Vol. 54, p1227-1232.

"If we have more information packaged neatly about ourselves surely that makes it easier for people to get hold of your identity."

"I think personally that there is a lot of technical complexity and dangers with having a centralised database."

"That data is being collected, is being amalgamated with other databases which are being brought in from all over the place, and ultimately will bring up a profile about you, which may be completely wrong."

A single piece of information may not constitute any invasion of privacy but when information is harvested from a variety of sources and amalgamated in a single database the picture is clearly very different. Hence it is not simply the storage of data that aroused attendees' concerns. Many were aware that the flow and transfer of information and construction of databases containing amalgamated information from different sources poses an even greater threat of misuse and abuse:

"Coming back to what you said about lots of information being held on different databases, what happens when all that information is put together?"

"It won't be correct will it, it won't be correct information."

"The possibility there is very great, the chance that some data held about me is in error is very high."

There is then a high degree of scepticism about whether data that is held about individuals is accurate. The last two comments are interesting because they illustrate two points; first the possibility that information may not be correct because it has been incorrectly entered or labelled, and second, because it may actually be spurious. It was interesting to note that many attendees told us that they used provision of false and misleading information as a means of protection and control against what they consider to be inappropriate or excessive data gathering and storage:

"It depends on the resource that you're dealing with as to whether you give the right information or not."

"I don't think I want anybody to have any information about me that I choose not to give them."

"Why do they need to know it anyway? Why do they need to know your correct address when you're just registering for a news web site?"

The widespread supply of false and misleading information has serious implications for the way in which such information might be used either now or in the future, particularly when it is used to make decisions that may impact on people's lives. The whole point of a database is to hold and make available accurate information; if this is compromised in any way then the value of the database is seriously diminished.

Media coverage of data gathering activity such as the recent debacle in the US regarding Google's disputed requirement to give up personal data to the government also sparked debate and sensitised attendees to the possibility of covert data gathering and usage. This resulted in many references being made to '1984' and George Orwell in the course of the discussions and also has the effect of heightening a greater awareness of the value of personal data and the unexpected and unwelcome ways in which it may be used:

"For me, as a consumer…I want to know that what I give, what data I give is not abused."

"It can be misinterpreted."

"It means that people can use it in ways that they want and pass it on."

Attendees were highly aware that their data is both valuable and vulnerable and easy to collect and they were keen that it should not be abused:

> *"If I buy from somebody, to me that's the end of the action, you've got the object I've got the money, we're doing a fair swap, why should they make money off of my information which is what they're doing."*

That information is valuable and should be protected was of particular concern to the SME community who are responsible for holding data about their clients:

> *"It's the value of the data, so like, being a wealthy person makes me more at risk because I have got something that somebody wants."*

> *"If you are an SME which is processing highly valuable data on the computer, then you are far more likely to be targeted to get that data, because the data on its own is valuable."*

> *"The entire value of their company is in that data, and not only that, but everybody else is interested in it."*

The story here is not completely negative of course; there were instances where attendees could see the benefit of data collection and storage, particularly where the same information needed to be provided to different departments of the same agency:

> *"I don't want to be submitting the same data time and time again for example to ten different government agencies. If I was unemployed and receiving child benefit, and housing benefit and assistance with my council tax and so forth, and I had to deal with all these groups, I think the list would soon add up. I wouldn't want to be entering the same data every single time I had to register, or had to deal with one of these routes, I'd want them to coordinate. Especially if I'm not computer savvy."*

And of course, it does depend on who is collecting the data and for what purpose:

> *"I think there can be tremendous benefit to companies having access to a lot of data about individuals but I didn't realise that so much information could be gathered together on me by the American government or, by say governments generally. So if they can do it, do we trust them?"*

It is interesting to note that although many attendees claimed in the discussion process that they would welcome the existence of effective fallback measures if something did go wrong, some, implemented by banks, served to reinforce a sense of vulnerability:

> *"I do like the fact that two of my credit card companies have written to me and told me that they are adding this fraud prevention, so if identity theft did occur then I have two different numbers I can ring to try and get it sorted. I'm glad that they've done that but on the flip side of the coin I'm worried that if they consider it such a high likelihood that it's probably going to happen, and banks believe it's going to happen or they wouldn't be doing it."*

It is clearly difficult for the banking and finance industry in particular to strike a balance between assurances of security on one hand, and increasing users levels of perceived vulnerability as a result of such activities on the other.

5.3 Control of Personal Information

A major area of concern that arose in the discussions was that of control over access to personal information. Attendees were concerned at the way this information may be used and gave several examples of incidents they had heard about or instances where they felt they had been the victims of inaccurate or inappropriate use of data held about them:

> *"The bank manager wanted to know my last four addresses and I gave her all the stuff. She was away a very long time and I thought there's something dodgy going on here, she came back and said 'have you stayed at blah, blah address in 1980 or whatever?' and I said 'yes' and apparently my name was up against a non-payment of Council Tax. She said, 'I'll need to go and make a phone call' and I said 'look I don't owe anybody any money except the banks, I've paid all my Council Tax.' She said I know that but there's a thing in legislation where if you stay in a flat and somebody before you has scarpered and left unpaid bills or unpaid Council Tax, that information gets passed on to the bailiffs…"*

> *"There was a lady refused a credit card because she had paid off her store card debt about 30 years ago and the debt was for £30 and she had written a cheque for £29.99 and she had a black mark against her name for 1p for 30 years, and she was a credit risk because of that. So you need a bunch of procedural safeguards to make sure you can find out what this information is and correct any flaws."*

> *"There was a programme on Radio 4, of people who were on police records for things that they had not done, it was really quite serious issues. It happens a lot and people are denied jobs, they don't get the job and it's because they've got a record, and they haven't really and again it's a case of proving your innocence, which is a very fundamental issue that we should not have to face."*

As previously noted, one method that is regularly employed is the practice of supplying false information, however many attendees were aware that this is a fairly blunt tool that cannot be employed across a wide variety of contexts. Attendees were aware that ease of collection of electronic data leads to requirements, legitimate or not, to supply increasing volumes of personal information to an increasing number of private sector entities and government and law enforcement agencies:

> *"The other problem though is with digital data, because it's easier to collect than hard copies of things, more and more people want more of it."*

> *"It's because of this wanting to know all the different things when you give a card, you know, invasion of our privacy, I try wherever possible to use money but it's becoming increasingly difficult."*

The lack of control over how information may be used increased attendees' sense of powerlessness and vulnerability:

> *"As soon as you've submitted data you can assume that data is no longer yours because you've got no control over how it's going to be used. When it's on a database you've got no control."*

> *"It depends on how it's used, who has access to it, why they can get access to it, how much the data is shared between different authorities, the parameters that allow that data to be shared…"*

> *"I don't see quite who is going to need the information that they are holding."*

However, although privacy is clearly an important issue we found many examples where attendees' behaviour belied this fact and they regularly surrendered their privacy. This was particularly prevalent in the case of failing to read privacy statements; almost all admitted to ticking a box to say that they had read a privacy policy when this was untrue. Most responded to this question with:

> *"Yes, all the time."*

> *"Doesn't everyone just tick the box that says they've read it?"*

> *"You rarely know what your rights are in terms of a privacy policy. Do you ever read the legal terms on web sites of any technology you use? I think that no-one does generally."*

For some ticking the box was simply the required next step in order to move onto the next field but others commented that they had absolutely no control over this process and hence it made no difference whether they had read a privacy statement or not because they wanted to complete the transaction:

> *"There is no choice, you can't go forward unless you tick it, and you can't argue the points in there."*
>
> *"It makes no difference, you can't opt out, if it says you have to tick the box to get something then you have to tick it."*
>
> *"You can't go through to the next stage [without ticking the box] if you want to buy it."*

Attendees also gave additional reasons for not reading privacy statements and policies that arose out of the discussions:

> *"Because they are to long."*
>
> *"Because they are written in stupid language for lawyer people."*
>
> *"They are very small."*
>
> *"A major issue I think is that they are written to confuse you."*
>
> *"Forty sentences and the jargon!"*

As exhibited in the statements above, human behaviour is generally neither logical nor consistent and such inconsistency in the realm of the desire for privacy and conflicting behaviour has not gone unnoticed. Cate[47] comments that although people claim they desire more privacy, their actions illustrate that they do not want to make much sacrifice of time or energy in obtaining it and our observations would support this.

Of those who had read privacy statements there were several occasions where attendees told us about statements that had put them off completing a transaction:

> *"It was about selling my data on and what they were going to do with it, sharing it with other parties."*
>
> *"Sharing information with third party organisations. Banks are very good at this, if you sign up for a credit card, part of the signing up is they share your information."*

Requests for excessive or inappropriate amounts of information had a similar effect:

> *"I refused, ages ago this was, a letting agency, I went in and said 'I'm interested in this house you've got in the paper,' they said 'can you fill in this form and we will tell you about it.' The form had so much data on it, you know, and that was their policy, you had to do it. They wanted where I worked, my personal home address, work address, phone numbers, bank account, who I bank with, so I refused."*
>
> *"Someone I know had sent me an Internet link to a web site that said you could get 400 free text messages a month. I can't remember what the name of the web site was. You went through and it said we want to use your information for this,*

[47] Cate, F. 1997. *Privacy in the Information Age.* Brookings Institution Press. Washington DC

> *we will hold it for a year, and we might send you marketing, and we might just send you random text messages. And I just thought 'nah', I don't care about 400 free text messages, I don't care that my friend wants me to sign up for it because they want to keep in touch with me. I'm not doing it."*

The statements above represent clear examples of attendees' attempts to exercise meaningful control and limit access to their personal information but this is often at the expense of not being able to avail themselves of certain goods and services. Although we are generally considered to be a card carrying nation it was surprising to note the number of attendees who said they would not use store loyalty cards, again as a means of exercising control over their personal data and privacy of purchasing behaviour. This was particularly true of the Nectar card and the fact that data would be sold on to a third party:

> *"But people do that inadvertently, like with a Nectar card, I don't think a lot of people realise that. I don't use one for that reason."*

> *"I don't use one either. Every time you swipe it everything that you've bought gets logged and they've got your spending profile."*

> *"I don't use one for the same reason but my girlfriend has and they do spot changes in your shopping habits, they're obviously using the data."*

Or when information might be amalgamated with other data sets:

> *"But you might get a Sainsbury's credit card and they can start linking it to your financial records, before you know it they could have quite a big picture of who you are."*

> *"You don't know who is using it do you? Or what for."*

Others were more wary about the actual benefit to the cardholder compared to the benefit to the supplier:

> *"Tesco club card points are worth about what, about 0.0001p or something like that. If you said to somebody I'll give you a penny if you give me all this personal data about you, who's going to be volunteering?"*

> *"They can find out things about you without, necessarily, your permission. For example those ticket machines at Bristol Temple Meads, the fast ticket machines you can program in… you select what ticket you want, put your card in and buy it. But when you first put your card in, a message pops up on the screen saying 'these are the journeys you have done recently, do you want to do one of them again?' They never ask you if they can keep that data."*

Although many attendees consider that they are well-informed about data collection in this context, and the possible implications, they did voice the opinion that others may not be aware of the problems, risks and dangers about how their personal information is handled, particularly the elderly:

> *"I think my mum and dad really don't think about those things. They don't think if I use my Sainsbury's card every time I go to a Sainsbury's, and because it is now that Nectar card thing, it is linked to forty-seven other stores as well, and so they can tell, you know, how many times you've been to Threshers and BP and where-ever else it is."*

Lack of control, covert and excessive data collection and vague policies concerning personal information all contribute to negative and sceptical attitudes. The avoidance behaviours described above do not bode well for the cashless society although clear information about what information is being collected at any given point and the way in which it may be stored, traded or otherwise used may provide increased positive perceptions of choice and control.

Almost all attendees wanted to be able to access data that is held about them and felt that this should be a basic human right but in this context they were aware that they did not know what information had been collected, how it had been used, combined, sold, which entities might be holding that information, how securely it had been held or even how they might gain access:

> *"On a personal level, I think yes, the ability to know what that data is about… I know theoretically you have a right to know now, but on a practical level it is very difficult."*
>
> *"You don't know what you don't know, you don't know how the data might be used."*
>
> *"We do have access anyway don't we, or we can get access can't we? Under data protection…?"*
>
> *"Do they store it, do they actually record it somewhere, do they ever delete it, and what do they do?"*

There is a clear requirement for greater individual control over how personal data is collected, stored, amalgamated and used, and a need for greater transparency of access to that information by the individuals themselves. It is also imperative to balance the removal of barriers to information access with new measures being implemented in response to contemporary security concerns.

6 Privacy, Confidentiality and Security of Health Information

As part of the NHS's £6.2bn IT upgrade a new NHS database is being introduced that will allow staff to access medical records wherever someone is treated. Clearly this has benefits to patients because the same information can be made available across different locations, wherever the patient happens to be. However the introduction of such a scheme is fraught with difficulties not least because it requires a shift in public acceptance and attitudes towards what is considered by most to be highly sensitive and private information that formerly was shared only with very few. Previously health information could only be made available to a third party with the express permission of the patient or in certain circumstances, by order of a court. In practice the introduction of the new NHS database means that such information could potentially be made available to many and this engenders varying degrees of distrust and has serious implications for the previously trusted doctor-patient relationship. However, some attendees cited examples where they could see the advantages of health information being more readily available and some felt it might be more accurate:

> *"Well if you need a life saving operation that depends on medical information it would be fantastic."*

> *"If you have a medical problem, you never see the same doctor twice. I mean we're lucky if we see them again, but if you've got all your details there, then you're sure that's all your medical details there."*

> *"The good part is that the person looking at the data is really looking at your data. At the moment sometimes they get confused and they're looking at someone else's notes. Hopefully online that won't happen."*

Not surprisingly the discussions around health information raised some very firmly held views. Attendees regarded medical information as highly sensitive and again, privacy and control of this kind of information were perceived as paramount. Issues of control concerned two areas in particular, first, confidentiality; who would be able to access health information and in what circumstances, and second, what level of control individuals would be able to exercise over information that was held about them, for example:

> *"If someone outside of my doctor's surgery can read all my medical notes that's terrible."*

> *"If the doctor's receptionist was your neighbour you can just imagine can't you, they'd be sitting there thinking, oh I wonder what they've got, I'll just look them up."*

> *"So there are cases, maybe you've truly got a triple blind and you cannot trace back data to the individual, but even then you probably can if you really want to. I think the problem is in the fact that the societal pressures for that are not there, unless as a society we decided that we must insist on anonymity."*

Again the human element in security, access and abuse of data arose, and not only in the context of electronically held data:

> *"But the Government has you on a databases, the health service, your doctor, and your security depends entirely on the integrity of the people operating those. It just takes one disgruntled employee and your details are sold … There's nothing you can do about it. You are wide open."*

> *"I lived in a small community which had a doctor's surgery, and had somebody working in that surgery who told most of the community about things that they shouldn't have. At the other end of the scale, I have a condition that I would*

really like someone in Newcastle to know if I was involved in a major car accident."

Concerns that such data might be misused are hardly surprising given that an individual's health details may contain extremely sensitive information that could have serious implications for personal or public life, educational or job opportunities. There is a good deal of debate as to whether patients should have the right to determine what and how information is recorded about them and most attendees saw this as an infringement of their right to privacy and confidentiality, for example:

"You have to be able to choose what data you want to be publicly available."

"I really dislike the fact that, actually, the doctors can keep all your medical records and you are not allowed access to them."

"I think that all that should be available is data that is needed for a particular medical procedure. I don't think people would mind about that and if it was just restricted to hospitals and doctors it would be OK."

In this context attendees also voiced concerns that there must be clearly laid out professional responsibilities to protect such sensitive information from falling into the wrong hands or from being abused:

"If anybody is going to look at that record it should be my GP and if this other doctor wants to look at the record then my GP should be able to say yes he can, but inform me that that exchange of trust has been made with someone else."

"Well some people I would trust to look at it and others I wouldn't, you know, I'd be very curious if I saw that…why is this government agency accessing that information? If you just built everything with an audit trail and an alert trail then…otherwise you're pushing it back on the citizen to be aware of what's going on."

"That information should be available to your doctor. Just your doctor, not any doctor, anywhere."

Almost all attendees were adamant that only doctors should have access to their health information and distrust of Government in the context of access to and use of health information was high. For some this distrust lay in the implementation of the database project and many attendees drew attention to the fact that they had little faith in Government's track record in implementing new IT systems:

"The government has a terrible record on IT projects, I thoroughly expect it to go wrong."

"I don't want governments running those sort of systems."

But most of this concern was focused on lack of trust in Government more generally and in particular how the costs of introducing such a scheme might be recouped:

"If we get a national health database, they will sell it on, because they need to pay for it. The likes of Gordon Brown will sell it on to pharmaceutical companies, and then they will sell on to other drug companies and what have you."

"I don't know what effect it's going to have on the government because nobody is going to trust the government anyway so they are always going to be at the bottom of the tree."

"The only snag is if the government is controlling this, would they only be using it for medical reasons? Are they going to sell it onto higher bidders?"

And hand in hand with this attendees expressed concern about how their health information might be used now or in the future and the potential for function creep:

> *"I am a drag on the state, on the health service because I have regular and expensive medication. Under the present system, my doctor could, if the Department of Health asked him, identify that I am a drag on the state… therefore, I must go to my doctor and say stop this medication, I'd rather die a natural death."*
>
> *"That's even worse if they start profiling your health risks."*
>
> *"And they will say that for fraud and insurance purposes that they are going to let insurance companies have access to your medical data, because, you know, when you buy holiday insurance you are supposed to declare every condition you have had in the last five years, and maybe you either can't be bothered, you don't want to, you don't feel that it is valid or whatever."*

Once again the problems and concerns of holding information on a central database came to the fore; most felt that such data could not be held securely and many attendees expressed fears about vulnerability, the value of their health data and the implications of this data falling into the wrong hands:

> *"Well it's open to the same kind of abuse isn't it? Basically it is open to people who are either hacking it just for the joy of it and replacing it with some sort of bizarre illness or, using it maliciously."*
>
> *"When the government holds all this health information on this huge NHS database, it will be hacked in to and that data will be sold to insurance companies."*
>
> *"It's sold to insurance companies because it is very, very valuable. Or insurance companies will actually employ people to hack in to it, because it is very valuable data to them, and they sell, they sell it to employers."*

Obviously the implications of health information falling into the wrong hands are very serious and the possibilities for redress or restitution are far more difficult to accomplish than in the case of financial or even identity fraud. Attendees named several entities they considered to be 'the wrong hands' and these included government, insurance companies and employers. Given the sensitivity of health information almost all attendees agreed that it is necessary to hold such details in the most secure fashion:

> *"It comes down to control of the data – I'd like to see lock down safeguards – it was taken for that purpose and should not be used for any other purpose."*
>
> *"For any type of record, be it tax or medical or anything like that, an ounce of prevention is worth a pound to cure and to my mind, I don't want there to be any possibility that I'm going to have to go to court and argue that I wasn't given a job because they saw my medical records and realised I had some kind of illness."*

Again, few thought that security would be possible on such a database although some did suggest alternatives:

> *"There are two ways of holding data, sensitive data. One is you have a central NHS database where all the, everybody's data is held in this central NHS database, and doctors have to log in to say that they are your doctor. And the other way is that you carry your medical data around in a smart card, where, if you want, if you want to have the doctor have access to it, you have to give the doctor the smart card."*

Others were sceptical of holding a smart health card and felt that it could potentially entail the same problems as a central database, in this case they were only prepared to hold a personal card that carried their data as long as the data was not held or stored elsewhere and they had control over the information that was included:

> *"What about the idea of having a card that scans. My own personal card that they kind of put information on?"*

> *"If you had control of what data was on that card…"*

A few attendees felt that a combination of methods to identify a patient may also be useful in avoiding medical errors:

> *"I think if we used an iris recognition combined with your medical notes, that would possibly be, well not bomb proof but fool proof."*

And although they were in the minority, some attendees felt that a central NHS database would make their medical details more secure:

> *"I actually think that having it stored electronically is a lot safer. Not that someone will want to nick my personal file, but if the surgery burnt down or whatever, that data is destroyed. But now, if it's replicated on four or five different servers to ensure integrity, I feel it would be safer in that. If number one copy got lost, then there would be a backup up and maybe I'll just lose 24 hours."*

Some attendees also suggested that access to medical records should be able to be tracked by the individual to whom they belong:

> *"You can't be secure but you can maintain logs, where everybody is thoroughly identifiable through a system, then you can recall everything that that person has done while on the system. In the NHS example you could find out who had accessed your medical records in the last month."*

It is very clear that there are some serious and as yet unresolved issues of security, confidentiality and privacy of patient information in the implementation of a national NHS database. Our findings suggest that if the service is to reach widespread acceptance the rights of the individual to withhold certain information, or even opt out of the service altogether, must be maintained and addressed with due consideration, respect and sensitivity. Very clear responsibilities for privacy and security need to be in place and these must be backed up with firm and honest guarantees.

It is also worth noting in this context that recent research by the NSPCC[48] on behalf of the Office of the Children's Commissioner (OCC) suggests that teenagers do not trust the confidentiality of the new national children's database. This is a Government initiative to be launched in 2008 in England and Wales that will gather records on 12 million children and their families and involves amalgamating data that is currently held in separate local databases into a central system to which 400,000 civil and public servants will have access. Clearly this raises serious concerns regarding confidentiality and the report suggests that vulnerable teenagers may stop using contraceptive, abortion and mental health services because information they provide may be shared with doctors, teachers, social workers and the police who will all have access to each others records. Understandably this is perceived by the potential recipients of the service as exacerbating rather than solving the very problems the system is being set up to deal with. It is apparent that there is a great deal of work to be

[48] http://www.nspcc.org.uk/Inform/Research/Findings/IThinkItsAboutTrust_ifega38731.html

http://www.publications.parliament.uk/pa/ld199697/ldhansrd/pdvn/lds06/text/60320-22.htm

done by policy makers and practitioners regarding sharing information with the required degree of security and attention to privacy before any such system will reach public acceptability and confidence.

7 Public Surveillance

In most circumstances individuals have the right and opportunity to choose whether or not they will engage with a particular technology and this level of control is fundamental to how, why and where such technologies are used, and under what conditions. However, public surveillance technologies, by their very nature, do not allow for any individual discretion in relation to choice, control, engagement, use, or any repercussions. Since control in relation to technology use is clearly a challenging and controversial issue, it is not surprising that strong feelings were voiced in relation to public surveillance technologies in the discussion process. The UK has the highest level of public surveillance in the world; approximately 20% of the world's CCTV surveillance is operated in the UK to monitor the movements and activities of its citizens. Although much of this activity centres on security, crime detection and prevention, we found high levels of concern regarding what is perceived as heavy surveillance and tracking of day-to-day movements and activities in public places:

> *"There's people watching me doing ordinary, every day activities which I consider as entirely private."*
>
> *"It is corrosive, being watched when we don't know and feel we're being watched has a very different psychological effect than being watched when you know you're being watched."*
>
> *"It's the feeling of being surveilled, is that a word? Under surveillance."*

Some attendees felt that reasons given for increased surveillance (e.g. control of terrorist activities, reducing crime) were dubious and this decreased their sense of trust that it was for their benefit:

> *"A lot of this stuff is being hyped up and marketed to us and sold to us as 'this will solve our terrorism problem, this will do that, this will do this' and actually there's two things about that. One, we know is who is to blame but it will not solve the problem they're telling us it's going to solve and so that reduces your trust. The second one is in any event, all of this stuff has to be after the fact, it is not prevention."*
>
> *"We're saying we're basically putting our trust in that technology to reduce crime. Now, there's no evidence that they've reduced crime, the evidence actually is that good street lighting is just as good at reducing crime as CCTV cameras."*
>
> *"I don't trust the government at all, they are paranoid about all this, why do they need to know our every move?"*

In 2004 the Independent Newspaper[49] reported that more than four million surveillance cameras monitor our movements in the public sphere such as in the streets, shops, banks, hospitals, car parks, railway stations, and the London underground (that alone operates 1400 cameras.) Awareness of the comparatively high levels of surveillance in the UK is increasing; indeed, the fact that the average Briton is caught on camera 300 times a day is even used in a current TV advertising campaign (Peugeot 207 cars). Our discussions revealed that such levels of surveillance are perceived to have increased in recent years with, for example, the enforcement of the London Congestion Charge and automatic car registration

[49] Independent newspaper (Tuesday 12th January 2004)

recognition camera systems that record the number of the vehicle and an image of the occupants that are linked to the Police National Computer. Many attendees found this unwelcome and were highly aware of how extensions of these technological capabilities might impact on their day-to-day lives and on society in general:

> *"In central Bath they've linked the cameras up to the database that tells the police if you've got tax and insurance and other cities are wiring themselves into the same computer. They're doing it ostensibly because they want to find out if people are driving without tax and insurance but the spin off is that they can actually trace a car wherever these cameras are operational."*
>
> *"An application of that of course is that if your vehicle is being tracked from A to B and they measure the time, they say 'well, taking your average speed, that means that you must have been speeding at some point' and that to me is a particular application where it stops people thinking. The brain is like a muscle and the less you exercise it the less intelligent we become as a society. The effect of having more things done for us automatically is that it becomes positive aggression. This speeding application means that you're not thinking about safety, it all done for you."*

As well as taking away individual responsibility for obeying the law such activities were seen by attendees to have far reaching implications for civil liberties, particularly in terms of how CCTV footage might be used by those other than the original gatherers of such data and a strong need for improved legislation was voiced:

> *"But things like CCTV, I don't think there's any law that stops my local petrol station for example sharing CCTV footage with anyone else who might be interested in it. It's theirs, they can share it with anyone they choose to."*
>
> *"Having a privacy policy is one thing but there should be national legislation that tells you what you can and can't do with say, CCTV footage."*

In an exploration of new techniques of control underlying our digital culture Hookway[50] introduced the concept of the panspectron to describe the use of CCTV surveillance to record activity in public places i.e. the case where no particular surveillance subject is identified in order to trigger an information collection process, instead information is collected about everything and everyone all the time. A subject appears only when a particular question is asked, triggering data mining in information already gathered to learn what can be gleaned in answer to that question. While in the panopticon[51] environment the subject knows that the watcher is there, in the panspectron environment one may be completely unaware that information is being collected at all[52]. We found that many attendees were highly distrustful of such data collection measures and felt that they infringed civil liberties:

---

[50] Hookway, B. 2000. Pandemonium: The rise of predatory locales in the post-war world. Princeton, N.J.: Princeton Architectural Press.)

[51] Foucault, M. 1979. "Panopticism," In: Discipline and punish: The birth of the prison. Translated by Alan Sheridan. New York: Vintage Books, pp. 195–230.

[52] Sandra Brahman Tactical Memory: The Politics of Openness in the Construction of Memory. First Monday Conference, May 2006. http://www.firstmonday.org/

> *"It means I can't travel from A to B in this country without a central computer logging my movements, I mean not an audit trail which somebody could dig into if they needed to if there had been a mass murder or something, but the idea that there is a central computer somewhere that knows exactly where I am. Effectively that's infringing on my freedom."*

> *"Mostly all these things turn up in hindsight, you collect all the data and then you realise oh yes we have all the data, we have this technology, why do we want this? You suddenly realise your whole life is just a chain of events which could be known to anyone."*

> *"Life becomes far too quantified, and measured and controlled. We are trying to over-engineer life and society and that's the trust issue I have, is that the way that society should go? To try and monitor where everybody is and you know, as you walk past the post office your pension gets credited to your bank account and then you use your phone to pay for a newspaper, that's over-control. I'm rather distrusting of that."*

Some attendees however felt that there was a certain 'safety in numbers' in that so much data is being collected about so many people they are likely to be able to remain anonymous. Others were not concerned about being caught on CCTV but were more cautious about who might gain access to the information:

> *"Personally, I feel comfortable with a degree of ordinary bog standard, run of the mill CCTV surveillance simply because there's so much stuff going on that nobody's really going to bother to track me because I'm in the noise, every individual is in the noise."*

> *"CCTV doesn't worry me at all because I know they're not going to be focussing on me. I don't get concerned about the information being there, I get concerned about the people who can access it."*

For most such levels and operation of surveillance techniques were perceived as extreme and many felt they were detrimental to societal values because they encroach on the private sphere and diminish a sense of control:

> *"I don't care that the neighbours see me walking down to Westbury-on Trim, but if one of them followed me around, and took notes, and published them for everyone else to read, and said well X has nothing to fear, this is what he did on Saturday and Sunday and Monday, and isn't it interesting what books he reads and where he goes and what he spends his money on, and all the rest of it, I wouldn't like, I just wouldn't like it. It's the loss of a sense of control over a private sphere that I most dislike, not because I have anything to hide but because it is a private sphere and it has a meaning in the sense of self to my children and to me and my wife. I think that is a very deep loss, the sense of a private sphere."*

> *"What we're all afraid of is the state saying we're in charge and we will let you walk around and do things that we will allow you to do, which is a hell of a difference from us being able to say I as an individual will walk down the street, I will drive my car, I will buy that bottle of wine, I will buy that book and it's none of your business a. what I'm reading, b. what I'm drinking and c. what I'm driving."*

It is interesting to note that we came across several examples of cultural differences in attitudes to public surveillance within the discussion groups; this tended to arise around acceptability/unacceptability issues of ID cards compared with public surveillance measures. Several attendees who had experienced having an ID card in other countries expressed

surprise that many UK citizens found this proposition unacceptable but apparently accepted the high degree of public surveillance carried out in the UK, for example:

> *"I've lived here for ten years but I lived most of my life in Scandinavia and all this discussion about international identity cards I think is a bit of a strange one because in Denmark everybody is up in arms about the surveillance cameras, here nobody gives a hoot, whereas there have been national identity cards for the past fifty years and nobody cares."*

Where surveillance technologies are perceived as impinging on the private sphere they are most likely to be met with resistance and objection. Our findings suggest that we are approaching the tipping point of levels of acceptability in the UK and the extension of existing measures should be introduced with caution.

7.1 Statistical Norms of Behaviour

Of particular concern was the notion that behaviour could be monitored to identify those that fail to fit a statistical norm or standard behavioural pattern. Such techniques are generally employed to identify threatening, damaging or criminal behaviour. Attendees felt that reducing behaviour to a mathematical probability was vulnerable to erroneous inference and results in an increased sense of guardedness and a decreased sense of individual freedom. The long-term impact of this was perceived to pose particular and unprecedented problems:

> *"You have to spend your time second-guessing what a system written by somebody who had to write a rule somewhere is going to make of what you're doing. For example there are smart surveillance systems that the railways use that detect people who are likely to throw themselves under a train. They detect that if you stand on the same spot and two trains go by you are at risk of suicide and they will send a security guy down to say 'why have you stood there and let two trains go by?' It's the same software that looks for rectangular objects sitting still in an airport lounge. That software is getting very, very smart and what it comes down to is statistical behavioural odds. If you just happen to feel like sitting there day dreaming, just supposing I felt like it, say I'm Keats and composing something, then I'm likely to be interrupted by this guy trying to save my life when I had no intention or thought of suicide anyway."*

> *"You buy something and you might be departing from the statistical norm given your profile on say Amazon, because you are buying it for someone else. So you have to be guarded all the time and think to yourself what am I signalling to what system by virtue of what I'm about to do."*

The long-term effects of such behavioural profiling were considered to have far reaching societal implications and there is evidence of a perceived mismatch between government and commercial interests and those of the public at large:

> *"For years now I've monitored what I write in emails because I know that everything written in email persists forever. Now you think of a world where kids grow up and throughout their childhood and adolescence everything they ever did or said, or where they went, or who they associated with, and what they bought is a matter of record…I don't know how we stop it but we certainly can't stop it without a huge amount of effort to make things anonymous and both government and commercial pressures are both quite happy for them to be a matter of record, they both want them to be a matter of record."*

> *"What it comes down to is that it is one of a whole incidence of things that are staring down at you in car parks, for instance looking at kids who might damage them. There is a pattern of behaviour that indicates that someone is about to*

> *break into a car, they lurk around, the patterns of movement, so lots of car parks have smart surveillance that looks for patterns of movement. And I think about all this stuff and I think you will become more and more aware of self censorship or you will start actually self censoring your behaviour because you think 'I don't want to trigger that system or that system.' People think it's all there for the public good and if we can save one life by this then we should surely do it and you think, hmm, where it all end?"*

Given the current political climate it is of course difficult to strike a balance between national security and the maintenance of civil liberties. If technologies continue to be developed and employed with the intention of monitoring large numbers of people they are likely to intrude increasingly into the lives of ordinary, law abiding citizens who in turn will increasingly find cause to object. It is therefore imperative that surveillance technologies gain increased levels of public acceptance and to achieve this they should be deployed in a responsible manner, under strict supervision, and with increased levels of public accountability and individual rights of redress for mistakes. This should be supported by a legally enforceable code of conduct and regulations, and clear explanations as to the proven benefits and advantages of current and/or increased levels of public surveillance.

8 The human element in security

However well designed or secure a technology may be, those people who manage, operate or input data are considered by almost all attendees to be the weakest link:

> *"Data cannot be secured because at some point people are involved."*

> *"I think it can't ever be secure, if you are storing information it has to be used by humans and accessed by humans and you will never be able to make the access to that information, however that information is stored, secure. You have to have doors into it and you can never completely secure the doors because of human frailty, human susceptibility."*

The technology itself was seen by some as relatively secure but as soon as people are introduced as operatives or users of data it was felt by most that any security inherent in the technology could potentially be compromised:

> *"I know encryption works very well, but it's the human side that lets the story down."*

> *"I'm sure you're aware that you can get round most technology, or if the administrator of the system takes a dislike to you, they can get access to the information. I mean at the end of the day, technology could be the downfall, or people could be the downfall, even if you have got a security policy in place, it doesn't mean someone can't break it."*

Most attendees were adamant that the human element posed the greatest threat to the security of data and voiced the opinion that it would be easier to gain unauthorised access from a human source than by hacking the data electronically:

> *"I think its sort of garbage in garbage out sort of thing. You don't need to hack the database. All it needs is someone unscrupulous who is inputting the data, and you've got incorrect data on the database then. There are too many issues."*

> *"If you want to get somebody's information, instead of hiring a hacker to break into it on a PC, you'll hire somebody slyly to go and bribe suitably low paid employees in organisations, anything from nurses to clerks, to low level civil servants."*

The comments above suggest that attendees were highly aware that the security of technological systems is always vulnerable to human action be it malicious, mistaken or accidental.

9 Improving data privacy and security

As noted earlier, the aggregation of data, data matching and centralised databases are viewed by many as a serious threat to the security of personal information. As a partial solution attendees suggested the following:

> *"We could resist the temptation to aggregate it, because keeping it in different places, a pain though that is, does make it very, very difficult for someone to do severe damage. Like my medical records are not joined to my financial re cords which are not joined to my purchase records, all this stuff is separate at the moment, no one person could easily could hack all of this stuff. If we could resist the urge to keep building ever larger lumps of personal data, that could be part of the solution."*

> *"I think it's OK as long as it's different information stored in different places."*

Other suggestions included having more control over the data:

> *"If we assume it's all going to end up in on place anyway then perhaps we should put procedures in place so that we have some control over what data is in there."*

> *"It's kind of working more in favour of the data holder than the person who the data's held on which is the wrong way round in the balance of power."*

Many attendees concerns were focused on lack of access to information that is held about them, the ability to correct inaccuracies, and the onus being on them to track down that data:

> *"There are organisations holding information about me, but if I don't know they're holding information about me, I don't know to ask them."*

> *"I want the right to get rid of it, or amend or correct it."*

> *"Other than in exceptional circumstances, you should be able to say I don't want to be on your database, take me off, or I'll stay on but you've got all this wrong."*

The need to control and manage collection and access to personal data is one of the most controversial and complicated challenges to privacy. In theory the ability to access information that is held about us is arguably inherent in the democratic process but in practice it is difficult to achieve. It is imperative to balance the removal of barriers to information access with new measures being implemented in response to contemporary security concerns.

9.1 Third party data management

As an aid to managing data flow and access we asked attendees whether they would trust a third party to hold and manage their data for them. Some saw this as an effective measure because they would only have to deal with a single source and felt this would enhance data accuracy and tracking:

> *"It could be my identity information because you don't want to have to keep producing identity information over and over again, at some point that becomes a real issue. So there could be a third party institution that I would trust to release only that information that was a legitimate requirement, and to track the use of that information in some way."*

> *"Now if I had one source which I could verify myself, then the chance of that data being in error would be very low. Now I don't know how you would create that trust but I do know it's possible because brands like HP come along and persuade me to trust in them so it is possible to create trusting relations with organisations."*

> *"If you can convince me to trust Amazon, you could convince me to trust somebody else to release to Amazon the details that they need to make a legitimate shift."*

Others were much more sceptical, couldn't see the advantages and would not trust a third party:

> *"At the end of the day they are always going to sell out to somebody who pays enough money aren't they? If the government says you've got to give us that data then they'll do it."*
>
> *"I wouldn't trust anyone to hold that data for me."*
>
> *"I'd let someone hold all that data about me if they were really rubbish and I could get in and change all the data myself. That would be better."*

The most negative reaction was to whether attendees would trust a government organisation to hold this data for them and this was met with a resounding 'No' except by a very small minority:

> *"I'd have more trust in a government organisation than a commercial organisation if it was set up properly."*

This suggests that scepticism surrounding third party data management is focused on the widely held belief that electronic data cannot be held securely rather than a lack of trust in a given third party.

9.2 Legislation

Opinions concerning solutions regarding safeguarding personal information varied considerably. Many were aware of the Data Protection Act and felt that it provides a degree of welcome protection but most also said that this did not go far enough:

> *"I think a good way around that is if somebody is going to hold information on you they are legally obliged to send you once a year a copy of what they hold, and you can check it and they bear the cost because they're going to be earning money on it."*
>
> *"I think, practically, if the government were going to legislate, then we would have to do certain things to protect data and stuff like that. As well as the Data Protection Act and things like that, I mean, the idea that government can legislate, you have to protect something on our systems like that."*

Most attendees were aware that the Data Protection Act could not protect them in dealings with entities outside of the UK and SMEs in particular raised this point in relation to conducting business outside of the UK. Clearly this point needs to be addressed in relation to this sector if we are to increase use and confidence of ICT mediated services amongst SMEs.

Although some attendees felt that legislation might be the answer many others recognised that this would have to be a worldwide rather than national solution:

> *"From the police force's viewpoint, we have a new legislation coming in that fails to recognise the international aspect of this crime which makes things criminal in this country but they're still not criminal in other countries."*
>
> *"One thing I wanted to say is there's no point in UK legislation because there is a global market, and if the US don't sign, then we're in a mess because we can only guard ourselves here. But there are no fortresses across the ocean."*
>
> *"We cannot control the world because we're on a worldwide web now and the laws in Bangladesh are not going to be same laws here so porn is quite*

> *acceptable over there. Even paedophilia in some countries may be acceptable so the British government cannot police the worldwide web."*

Others felt that any legislation that could be introduced would be lagging behind the speed of technological change, or would not go far enough:

> *"The other thing is that the technology is moving so fast they can't legislate, or by the time it is legislated for it's moved on tenfold."*

> *"The Fraud Act which is yet to receive Royal Ascent but will be doing so this Autumn, covers some of these issues and I haven't read it in depth but it does make some changes to how the Internet works and what is needed but what it doesn't do is address the international boundary problem again. It doesn't matter how much Europe decides to do something, if it's some guy in outer Mongolia … there's not a lot you're going to be able to do besides starve his goats, so there is an issue there."*

People are aware that personal information is collected and used without their knowledge or consent and inevitably the question of who owns that information will arise and will no doubt be challenged. We feel that in isolation, it is unlikely that increased UK legislation concerning individual rights will adequately resolve these problems because security and privacy of information is often beyond the control of the individual. People do not know what information needs to be protected or why and this is largely due to the fact that this is likely to change rapidly over time; they do not know what information is held about them, by whom, for what purpose, or how it is being used currently or may be used in the future. Since personal information is collected and held outside of the UK it is also outside of the control of any UK legislation. A variety of measures need to be put in place that address individual and institutional rights, responsibilities and accountability and take account of the diversity of aims and motives in limiting, gathering and processing personal information.

10 Use of public access terminals

The balance between risk, usefulness and convenience figured strongly in the discussion around the provision of public systems, i.e. systems in public spaces that provide access to the same services that might normally be accessed from the home or office. The most obvious public space service provider is the Internet café, where convenience and ease of use are key benefits. However, even when such services were used for what would appear to be low risk applications attendees voiced concern and distrust:

> *"I wouldn't even check my email from a public access point, it's not secure."*
>
> *"I wouldn't use anything in a public space that required me to authenticate myself in any way to use it. It can all be traced."*
>
> *"I would have liked to be able to use the web at home, it feels safer, but if I've got no other way I'll do it from a public access place and worry about it after."*

Although attendees generally rated home use as more secure than access via a public terminal not all were worried about the perceived threats that use of public systems presented, a few felt that it was as safe as using the Internet at home:

> *"I don't know that much about it but I think it's as safe going on a site from home as it is going on in a public access place."*
>
> *"I thought that as long as it was all secure and that you logged off at the end, I didn't think anyone could come along after you and see what you'd been doing and get your details or anything."*

Other attendees made crude risk assessments in terms of benefit vs. potential loss. For example, some attendees felt that an Internet café was safe to use when checking emails but not for making credit card payments or contacting their bank:

> *"It's more dodgy using it in a public place and giving out your credit card details. I don't mind using it for checking my emails or looking up something on the web but I don't like using my credit card."*
>
> *"I'd only do that from home, I wouldn't check like my bank stuff from a public terminal, in an Internet café or a public space."*

A minority of attendees blamed problems on access via a public terminal when the event was equally likely to occur via a private system:

> *"I've had problems with my credit card, I think that might be linked to transactions over the Internet. I don't really worry about it because the bank takes care of it, well they have on the two occasions where it happened. It was definitely related to doing this in a public space because I haven't got Internet access at home."*

This attitude towards cautiousness suggests that the protection against fraud that banks actively promote is not entirely mitigating the risks for all attendees in all contexts. What is more likely is that those attendees recognise that their loss could be greater than just financial if their personal information is compromised, e.g. their identity is stolen. Alternatively, it could be that attendees are taking heed of the bank's warnings about using public systems to access bank account details[53].

[53] Example of security warning issued by bank regarding Internet cafés, http://www.natwest.com/global_options.asp?id=GLOBAL/COMMERCIAL/BANKLINE/GETTING_STARTED/SECURITY

There is clearly also a relationship between convenience, trust and cost related to use of public access terminals:

> *"I go where it's most convenient, I've been to the library because that's closest and it's the cheapest as well. It's not so much to do with trust as it is to do with convenience. Thinking about it I would feel more trusting to go into a library than I would to go into a café."*

Public systems by their nature are shared, and this action of sharing is at odds with values of trust and privacy. Attendees were generally well aware of the protection provided when accessing their bank, signified by the presence of the padlock in their browser, and accepted this as a sign that their information is protected, but this did not appear to allay their concerns about risks in the sphere of public access.

The location of a public system also had a bearing on how attendees evaluated risk. Access via a library terminal was viewed as more secure than access via an Internet cafe:

> *"I'd rather do it at the public library than an Internet café because it just feels safer, I don't know, probably people with evil intentions can't get to the mainframe systems of a library as easily as they can in an Internet café where I don't know who owns it or who is running it or anything."*

> *"I would not use an Internet café abroad. It's too easy to capture my information. It's not worth the risk."*

> *"Maybe I'm just being naïve but I do feel safer using it in a library than in some other public space."*

This suggests that it is not the technology per se but the way in which the technology is managed that makes a difference. Some attendees believe that a system operating in their own country is less risky than one operated overseas, and yet there was no indication that they considered the Internet in one country to be different from another. Familiarity may have a role here in that we also found that attendees were happier dealing with on-line organisation that they recognise (brand value) and that they could (at least in principle) contact in person to resolve difficulties.

Some attendees had experienced problems when using public systems and this had a negative impact on repeated or continued use:

> *"Someone used an Internet café PC after me and emailed me. It was not offensive but it was an invasion of my privacy."*

> *"I had a similar situation and now I never use Internet cafés."*

As we have seen before, attendees actively balance risk against convenience, and pay little regard to the claims made of the security technology they use. Public systems are seen to be of higher risk, but this may have less to do with the technology and more to do with the association with physical private and public spaces.

11 Mobile and location based services

The use of location based services via Bluetooth[54] (and similar) wireless communication technologies such as a mobile phone or other portable device raises many issues that relate to privacy, trust, authentication and identity. However, use of such services also introduces an added dimension, that of tracking, profiling and unsolicited contact, i.e. information being pushed at users rather than pulled. Bluetooth enabled phones, by virtue of the way the technology works, can automatically give away personal information including identity and location and many attendees were uncomfortable with this and while they could see some advantages they were also aware of the disadvantages this might bring:

> *"There's good and bad sides, at the moment parents can track the location of their children which sounds like a very good service but then again it could allow other people to track their children which is then a bad service; there's two sides to the coin."*

> *"You might decide that somebody who may be accused of something but may not have any evidence against them, but you will still actually try and track them electronically and in some ways that's abuse. You can see why that might be a good thing but it's also potentially a bad thing as well."*

> *"They can locate you down to within a couple of hundred yards and that's in a city, and the new ones are coming with GPS so they can locate you down to ten feet if they want to."*

The provision of mobile services, i.e. typically web-based services that can be accessed from portable devices like mobile phones, PDAs and laptops, has received much attention in recent years, particularly in relation to location based services[55]. A key characteristic of mobile services that effectively changes the landscape is their permanent connectivity. For example, mobile phones equipped with GPRS[56] can provide a permanent data connection between device and service provider, and subsequently through portals to the Internet. This means that the physical control of disconnecting a PC from a service (e.g. when terminating a dial-up connection) is no longer an option. In this context some attendees were unsure as to whether a Bluetooth Internet connection could offer them the same safeguards as a PC connection:

> *"With the Internet you're assured that with your own PC that you've got some kind of firewall in place and virus protection and you feel secure in using it and you've got it all set up, whereas with Bluetooth it's so much the unknown. Whether that's just psychological and whether Bluetooth is as safe as a firewall protected computer we just don't know."*

> *"I would be concerned about security in that if this is on while I'm roaming around someone could hack in and use my Bluetooth."*

Location based services are typically targeted at individuals who need ad hoc access to information that is specific to where they are, e.g. tourists, students and youngsters who rely on or choose to use mobile devices and a variety of communications methods (voice, data,

---

[54] Bluetooth, http://www.bluetooth.com/bluetooth/

[55] Mobile Services: Functional Diversity and Overload, Sørensen et all, Department of Information Systems, London School of Economics and Political Science, United Kingdom, 2002, In New Perspectives On 21st-Century Communication

[56] GPRS (General Packet Radio Service) is the world's most ubiquitous wireless data service. It is available on GSM networks and based on IP (Internet Protocols) thus supporting B2B and B2C applications.

SMS) in preference to traditional fixed line telephony. To an extent the increased popularity of mobile devices is a direct result of the services and convenience they offer, especially in a mobile environment. Some attendees could see the value of mobile services in novel contexts:

> *"I can just imagine using [Bluetooth messaging] on a ski slope with a ski partner, it would be great because of the close proximity."*

However, because Bluetooth operates over a short range and means that individuals using such devices are likely to be communicating with people who are visible to them many failed to see any benefit to this facility:

> *"Do people actually go around sending messages to each other? It's very much about how stings work; they're in close proximity before robbing you."*

> *"I struggle to see how I'd use this feature and I'd just leave it switched off."*

The comments above highlight the importance of developing technologies that are relevant to users lifestyles since those that are perceived to increase vulnerability without any perceived advantages to the user are unlikely to reach high adoption and usage rates.

11.1 Tracking and unsolicited approaches from service providers

Attendees were particularly concerned about tracking activities that extend beyond what might be considered 'related interests,' for example where a pair of shoes bought from a shoe shop still has an embedded security ID tag enabled when the customer leaves the shop. This means that others could read that tag, record and profile movement and correlate identity through other purchases and payment methods. Most attendees were uncomfortable with this kind of activity:

> *"I think that's too much. Wal-Mart has started doing it so you could probably see it happening."*

Attendees had mixed reactions to retail outlets tracking customer behaviour as they move about the store in order to target them with marketing information:

> *"It depends on the person, I think everybody now, it's got to the point where they just tune out advertising, like you're watching TV and it's just another ad, and another ad, you're not really paying attention to it, it's just flashing in front of you so you can choose to ignore it, it's up to you."*

Some location based services have the ability to track buying habits, including where purchases are made, and some attendees felt that this was an infringement of privacy rights and intrudes too far into the private sphere:

> *"I think I wouldn't like someone to know where you are at a specific point in time or what you're going to do, what you're going to buy."*

Location based services delivered via mobile devices mean that information can be pushed at consumers rather than pulled and many found this annoying and an invasion of privacy:

> *"Personally, if it came up every time I walked into [a store] that would annoy me. It's like someone attacks you on the phone as you go in the door."*

However, attendees thought that this was more acceptable in the case of permission-based services:

> *"I do like the idea of enabling the phone so that it tells me about special offers, etc. That's OK because I'm doing it permission based. It's not just broadcast. I know there's some element of trust because you have established that you buy from them."*

The problems that location based services can bring in terms of infringement of privacy are well recognised but poorly addressed to the extent that some civil liberty groups are raising questions about the potential cost to privacy, permitting lifestyle choices to be on public view[57].

11.2 Perceived risks and side-effects

Many attendees were well aware that systems that rely for their operation on location information are already in use, for example the Oyster Card scheme operated by Transport for London[58]. Attendees were aware that such schemes have the potential to infringe privacy and for many the information gathered was considered to be tantamount to covert surveillance and most found this unwelcome:

> *"Of course, there's Oyster cards where people can find out about crimes that have been committed and where people are at particular times; that can be for good and for bad and the government and security services may have a different view of people that are using those services."*

> *"I don't like the fact that somebody could actually find out where I am or where I've been, unless it's my choice. If I want my family to know, or my employer to know where I am at a certain time then that's OK, but if I don't…"*

Most attendees were concerned about issues of control and use of the data being gathered about them:

> *"I think that the major problem is that you're not in control of the information afterwards, once somebody else has this information they abide by their own policies so you don't want to distribute your information to certain people; you're not in control of that anymore. If you want to tell someone where you are, you can do so at your own will but if someone else knows where you are they can tell whomever they want to."*

Alongside issues of control the possibilities for function creep also arose in the discussion process. Location information allows individuals to be tracked and their daily habits (e.g. shopping) observed and predicted. For example, by recording the Bluetooth identity of a person each time they enter a store, and correlating the time of recording with images captured from a CCTV surveillance camera, it is potentially possible to associate a name with a facial image. This could be perceived as a serious invasion of privacy as far as the individual is concerned as they go about their day-to-day activities:

> *"It's not only your location, it's what you're doing with your time, the government or other people may not agree with what you're doing at some point, like Google for example, they're stopping the use of the Internet in China, ISP's giving out information to US governments. That's what is going to happen in the future, these are things that the government are going to be interested in finding out about people for what they see as good purposes, but they may not actually show very much, they might find more false negatives than positives."*

Instant messaging and mobile multimedia are clearly applications designed specifically for the person on the move. Depending on the nature of the application, they target different markets (e.g. SMS, remote email, rapid deployment emergency services). 'Social networking' is particularly popular with the younger generation, where the "TV set is no

[57] Big Brother or friendly helper? http://news.bbc.co.uk/2/hi/business/974999.stm

[58] Transport for London Oyster Card: http://www.tfl.gov.uk/tfl/fares-tickets/2006/index.shtml

longer the first thing they turn to after a day at school"[59], but as we discuss elsewhere in this report, it is not without risk. It was interesting to note in the context of whether attendees considered themselves to be more at risk in the physical than the on-line world, some felt that with the advent of location based services the electronic capture of location information would be so commonplace that the two worlds would converge:

> *"You're actually in a particular physical environment and you're more at risk from an electronic attack by the virtue of being in that particular location."*

By their very nature location based services are not anonymous and rely for their operation on the fact that devices are permanently connected and this means that users may inadvertently give out more information about themselves than they realise or would choose to do. Many attendees were surprised at how much information can be discerned without either their consent or choice:

> *"Well, certainly a concern for me would be that if I'm within easy reach of a network, whether that network can be used to download information from my phone."*

> *"I'm a bit worried about being actually identified."*

In order to avoid being recognised and to protect their identity some attendees were prepared to adopt a pseudonym or similar on their device. The opportunity to masquerade under a false identity appealed to some:

> *"I quite like being anonymous, until I know what someone wants from me. On my cheque books I always have 'name' I never have Ms or Miss or even gender."*

> *"You might like to choose a name that gives away just a little about yourself – the more exciting things."*

> *"The fun of a pseudonym is that you can then inject some of your own personality into it without actually being identifiable."*

Few attendees had extensive first hand experience of location based mobile services but most were aware of the potential for giving away information unintentionally, even if they were not aware of the extent of the information could be gleaned from their usage and location patterns. Those who did have experience of these services tended to use them only when they felt they were essential, preferring instead to switch them off when not required. This highlights the importance of developing technologies and services that have a high degree of inbuilt appeal i.e. those that enable consumers to do something that they couldn't do before, or make it easier to something that they could do without ant increased risk or added vulnerability.

[59] Show and tell online, http://technology.guardian.co.uk/weekly/story/0,,1720763,00.html

12 E-Government and Public Sector IT

E-Government is seen as central to reforming and modernising all public services and, with currently 62% of the population regularly using the Internet[60] the UK is viewed as a country that could greatly exploit electronic service delivery and in aiming to make all its services available electronically by 2005[61], the Government is attempting to exploit this potential.

The key benefits that are expected to be achieved as a result of the electronic delivery of services are:

- Wider participation (also known as e-Democracy), reduced social exclusion and improvements in information sharing between services and agencies
- Greater variety, choice and convenience of access for customers
- Improved speed and efficiency of the processes which underpin services

As e-Government matures the means to engage with, and empower citizens through e-channels becomes even more important. The emerging Transformational Government strategies hold the technology put in place in the e-Gov drive as central to providing an empowering infrastructure for citizens, communities and businesses to become more involved in the democratic process[62].

Therefore, it was important to consider e-Government usage and attitudes within the discussion groups because if citizens are not aware of, or "trust" public sector IT, the strategies proposed to revolutionise Government practice over the next ten years might be, at best, over-ambitious, and at worst, a significant waste of taxpayers money.

12.1 Citizen Engagement with e-Government

Findings from the groups would suggest a strategy that is perhaps trying to run before it can walk. One of the main issues that emerged was that of quality, in comparing Government sites against those in the commercial sector:

> *"Dreadful – they've all got different styles, webmasters. And just to find the information you've got to go so deep."*
>
> *"Six weeks, and two letters coming in, to file my annual returns. And it would have only taken me a couple of hours to walk there and back! That's happened for the last 3 years in a row - crazy."*
>
> *"We work with health and social care organisation, and every single organisation has a different looking and functioning web site. Every single one."*

The lack of consistency is something that has arisen time and again. General opinion is that both look and feel, and the functionality available, are below that of a comparable commercial site. However, certain services did get positive opinions about them:

> *"What's the best government one? I know what my answer is – DVLC, they've got it absolutely spot on. It's a new one; I filled in my details and got a tax disc in the post in a couple of days. It really works."*

The reason for this success is effectively summed up in a very brief quote:

---

[60] http://www.citizensonline.org.uk/statistics

[61] http://www.number-10.gov.uk/output/Page2795.asp

[62] http://www.cio.gov.uk/transformational_government/strategy/index.asp

"It's a single product isn't it, difficult to screw up."

This concept is one that is central to the problem of e-Government, when looking at evidence from the discussion groups. E-Government is not about delivering a single system, it's about linking up a huge variety of systems through, ideally, consistent interfaces. It is apparent that this connectedness between systems is not working and the impact is telling:

"We have to submit all our details of quotas and things through the DEFRA site, right. But when the bloke from DEFRA comes out to see me, he has a clipboard and a fax. Once he dropped in on the ground, it got mucked up, and then he couldn't read it! So, why do I have to do everything online when it's obvious they're not using it online themselves?"

"I guess the fundamental point is the government is pushing this on everyone else, and they haven't got their own house in order."

And as a result of these observations or worse, negative experiences with public sector IT, attitudes toward such systems become unenthusiastic very quickly:

"Why should I submit my details online? It's only saving work for the Government. What's in it for me?"

Negative experiences and their significant impact is something that runs throughout the findings of the project, whether this is to do with commercial systems, security, training or public sector IT. A single negative experience can result in a severe attitudinal adjustment and one that invariably results in mistrust and complete disengagement with that particular service.

12.2 Local e-Government and Awareness

The 'what's in it for me?' concept is something that any IT system vendor needs to address. In the case of public sector IT it is especially important because, in particular for local e-Government, there is little financial incentive for engaging with these systems. The message coming from the quote below was certainly not a common one arising from our study, however, it is extremely significant:

"We moved house recently, and we had no idea about when bins were collected, recycling, etc. I went online to the local authority site and found it all. I wonder what we would have done prior to this information being online."

As we can see from some of the quotes about use of e-Gov services, the systems where there is some sort of financial incentive, such as tax returns, are tolerated as attendees can see that if they manage to successfully return online, they will save money. However, for the majority of local authority services, where such financial incentives do not exist, they will simply not use the service. The quote above clearly demonstrates that when people can see a value in the services the system provides, they will engage with it, and feel positive about it. However, this is not something that can be approached in a prescriptive manner because it is not until they have a need that can be fulfilled by e-Government that they will see its value.

12.3 Online voting

One final issue that was examined within the groups, related to both e-Government and wider issue of trust, was that of online voting. When quantifying opinions, there is little to choose from between those who are pro online voting, and those who are against. Our discussions revealed an almost a 50/50 split. In examining the split further, it is apparent, unsurprisingly perhaps, that the young, and IT literate are the most positive toward the concept.

General concerns from people to be negative toward the concept centre around security issues; how can you ensure someone only votes once, who is responsible for the infrastructure, etc.:

> *"I'm pretty bothered about it really, I just can't see how it could be made secure, that's what worries me, and there isn't anything the government could tell me that would make me believe that it was. I'd prefer to go and cast my vote at the polling booths than use the web."*

However, those positive to the idea share views regarding convenience, and a positive skew to the voting demographic. They believe that online voting could be a means to engaging with groups who current aren't able, or can't be bothered, to engage with the democratic process:

> *"I can see that more young people, who don't vote because it tends to be older people who vote, and you would get 18-30 year olds who are less likely to vote than older people, they are technology literate, a lot of them have access to technology in the work place and things like that. So even if they didn't have a computer at home, they might be more inclined to [vote]."*

In conclusion, it is worth noting that the Financial Times recently reported a study by Accenture,[63] that suggests that the UK is still lagging behind other countries in persuading the public to use online and other electronic forms of government services, despite multi-billion pound investment. According to the study of twenty one countries: "Take-up of online services continues to be a real challenge for the UK, in spite of a relatively high proportion, by international standards, of households having an Internet connection." The report shows that only thirty eight per cent of the population used an e-Government service last year, essentially unchanged from the year before, and the UK had the highest percentage of citizens who used the post to contact government among the twenty one countries surveyed. This compares rather unfavourably with Canada for example where sixty eight per cent of citizens used e-enabled government services.

Whist we recognise that the introduction of last November's Transformational Government Strategy is attempting to address these problems by setting up directors whose task is it to design services across central and local government boundaries and between departments for particular groups of customers, there is clearly a long way to go.

[63] Financial Times, Monday May 22nd, 2006

13 Awareness and education

In understanding people's attitudes toward online life and their perceptions of "trust" it was also interesting to examine issues of awareness and education; whose responsibility is it to promote online awareness and what methods could be used to achieve it?

Trust is only necessary where an expected outcome cannot be guaranteed; otherwise the need to trust becomes obsolete[64]. Hence attendees use of the term 'risk' in describing ICT mediated activity would seem to signify varying degrees of uncertainty about the outcome of such interactions and this uncertainty is interpreted as 'risk.' One particularly pertinent element of uncertainty in the context of ICT mediated activities is the lack of knowledge or expertise to make decisions that will increase our belief that we have taken the necessary steps to protect ourselves as evidenced in the statements below:

> *"Well I do feel when you get these screens that say 'you are about to' you know those messages, and because I don't really understand what they're talking about because I'm just not sufficiently computer literate to understand, then I probably think I am running a risk and I'm too ignorant to even know what the risk is."*

> *"I have a virus check and it pops up and it says 'you are at risk from an incoming…' and what it means is that the application that I'm using is wanting to contact the Internet, you know it might be something perfectly harmless and innocuous or it might be that someone is trying to come in and read my keyboard and steal my password and my money, if I had any. But that's the thing, it's that ignorance and you don't know whether to say 'accept' or 'decline."*

From the highest to the most basic level, pervasive computing brings many challenges, not least of which is how to determine the right questions to ask and where to find the answers, and this was never more pertinent than in the field of education about the potential risks associated with use of such systems. If we do not know what the risks are, how can we protect ourselves against them? The recent Get Safe Online Survey[65] found that fear of crime acts as a barrier to people going online with nearly a quarter of respondents too concerned about e-crime to bank online, almost a fifth would not shop online and one in six had been put off logging on altogether. Most importantly nearly three quarters of those questioned said they needed more information to arm themselves against online threats. Our research suggests that the figures may in fact be higher; a distinct and urgent need for awareness and education arose again and again across all our workshops:

> *"If we educate ourselves, if the government makes it a priority to educate people, then we won't fall foul quite so much."*

> *"Education is the answer, society is more educated about what the risks are and being more streetwise, people don't tend to walk down dark alleys on their own these days, but they'll do the sort of metaphorical equivalent on the Internet."*

> *"With regards to the Internet…I don't think we can police it, so we have to educate, it's so intangible."*

Early discussions brought about an interesting additional viewpoint – is awareness the issue, or should we be focussing more upon the responsibility of service providers, manufacturers, etc. to produce equipment and products that are secure? If this was the case, ultimately the

[64] Giddens, A. 1990. *The Consequences of Modernity*. Stanford University Press: Stanford

[65] Op cit

end user does not need the commonly expected level of awareness necessary to achieve secure communications online:

> *"The responsibility is with the ISP, it should be legislated that the ISP have a duty of care to the customer."*

> *"People who write the operating systems they make money out of us when we buy a laptop or a PC. There is a huge responsibility on them, if they want to make money from it, to protect, as much as possible, the software they've got… You make money out of putting software on this system so you should be trying as hard as possible to make sure it isn't hacked."*

> *"I think you ask the question, education, where does it start? It starts in the home, schools have a responsibility but I think we all have responsibility but also the providers, the software and hardware providers also have a responsibility to ensure that the right level of education is given when they unpack the box, but I think education starts from the home."*

An often-used analogy was that of the motorcar:

> *"If I make a car and sell a car I have a responsibility to make sure the brakes work, etc. before I sell it. What I am saying is that if I sell some software I should have a responsibility to ensure it is safe."*

This view emerged from a number of different groups, that is, the fact that when you drive a car there are certain expectations of security, placed upon both the manufacturer, who should provide a road-worthy vehicle, and the legislators, who put measures such as MOT certificates, legislation around insurance, etc. in place. However, while this analogy works to a point, it fails to recognise the responsibility of the individual to ensure adequate insurance and roadworthiness through regular servicing and MOT tests.

Attendees also acknowledged that the software industry, and the Internet, is hugely more complex to regulate than the car industry:

> *"This is a fundamental problem with IT – it's simply not a consumer product, even though you can buy it in Currys, or wherever. Software isn't really a consumer product that can be installed, set up and managed by the uninitiated, and the Internet and the web are places you should not go without training."*

> *"Everybody is a stakeholder in this problem, everybody stands to lose or gain depending on how well this problem is resolved and I think it's probably too much to ask that there should be a concerted effort, but there should be an obligation by everybody to ensure that all parties in a transaction are aware of the risks involved. We are not just talking about understanding that using a computer could be a dangerous thing, you need to look at the education of the supposed security professionals and IT professionals who design the technology, design the applications, design the infrastructure."*

> *"I think the key phrase here is 'fit for the purpose,' you're selling goods to people that are not fit for the purpose. Before the Internet happened and somebody just wanted to run a programme at home it was perfectly fine but if you connect to the Internet now and you are not aware of the threats out there you can be infected within minutes."*

The issue of legislation arose a number of times, but the better-informed members of the groups always returned to the issues of a global marketplace and the anonymity of the Internet:

> *"Another problem with the Internet is that it's not possible to control it. The essence of the Internet provides everybody with the freedom to express their opinion. People around the world can do what they want… If you try to control it*

> *you have to fight with the essence of the Internet… It has happened many times – the American government has tried it many times and the number that object means they have to go back."*

While legislation is viewed as a naïve tool to control misuse, it is generally agreed that a well-informed individual is generally a lot safer online than someone new to this 'cyber world' without being aware of the risks.

Therefore, we returned to the question of who is responsible for promoting awareness of the dangers of going online, and how can people best be educated?

> *"I think everybody, or as many people as possible, people who sell computers, people who sell the software, people who are providing the online application of whatever process it is, and the end user should all be responsible for it."*

> *"You've got to meet them half way, you can't expect the people that are amateurs at something to put all their effort into having this education. They don't have to do that when they buy other products, not to that extent and I know it's a complex product so it's difficult, but we should try and make it as easy as possible for them."*

> *"When you plug a PC into the Internet, then it becomes a different beast entirely, therefore, surely it's down to the Internet providers to have some input in this because surely they are the ones who are pipelining information to us and from us and therefore they are the ones that should carry some of the responsibility."*

Interestingly, a lot of workshop attendees have stated that they do not feel at risk themselves because they are aware of the potential dangers (however it should be noted that in recruiting people to attend focus groups on IT security one must assume a certain bias to those interested in the topic!). However, they do feel that 'the public' have a need to be educated about the risks in going online and carrying out aspects of everyday life therein:

> *"I'm not worrying about my use of the Internet, what I would worry about is the exploitation of the more vulnerable or more naïve people using the Internet."*

The responsibility for providing that education is an interesting issue to visit. A common view in most groups was the onus being on individuals to become aware and educate themselves:

> *"The model back in the 1890s was 'buyer beware' and that is still the case in certain aspects. If you have a leak in your house and you need a plumber, who do you call in? I had an electrician masquerading as a plumber!"*

But there was general agreement that there was a role for the Government in making people aware of the risks:

> *"The first principle of government is to protect the vulnerable and I think we are vulnerable, the Internet is in its infancy isn't it? We're all moving into this new age and I think why not, the government should give info, not hound us in the same way as junk mail is hounded, but make it available."*

> *"The government are the ones who should educate – they aren't a private company and therefore there is no bias in what they are providing."*

> *"Ultimately it's the government that are setting the framework and the strategy to make education successful, but that means the government has got to be open and honest about it, they've got to be clear, they've got to send out clear messages, unambiguous messages, teachers have got to be informed. Often teachers aren't informed, parents have got to know more about technology, often they don't because of the era they were growing up in I guess so there's only a small section of society I think that really understand the risks involved."*

> *"I think government does have role in this. Remember a few years ago you could buy white goods without a plug attached and on safety grounds they said right you're going to have a moulded plug because people are getting electrocuted because they can't fit plugs properly. The same sort of sequence of events could apply to computers, they have to have security built in either in the hardware or the operating system so these threats are no longer as dangerous to the people."*

However, somewhat in conflict with that view, the level of awareness of Government and media initiatives to promote knowledge about the risks of being online (for example, the "Get Safe Online" web site[66] and newspaper inserts) was extremely low, and those that were aware did not hold the efforts in high regard:

> *"Certainly in the IT industry they viewed it as yet another initiative going nowhere, wasting money saying the same things. The barriers are there and the government has a responsibility to educate, but perhaps we don't want to listen!"*

This data brings into question the value of mass media in communicating issues such as education and awareness. While the media are undoubtedly effective at reporting 'news', this is information that the reader may not know they need to know about! Additionally, the nature of the media, and its relationship with the Internet was brought into question by one attendee who had worked at the BBC for over 20 years:

> *"I think the media are romanticising a lot of these fraudsters. There was that guy in Newport recently, who came back and ripped some more people off. And the media made him out to be a modern day Robin Hood! …The press and the media is such a powerful thing, TV's biggest threat is the Internet – it's a vicious circle… the media has a part to play and I don't think they are castigating the people who are doing it."*

When asked about what methods people considered to be more effective than the mass media approaches, it was clear that information communicated by a peer or facilitator was more valued than that from a newspaper insert:

> *"Business in Focus and things like that are available for businesses starting up. Varying quality I know but they are there. When I was starting up the only reason I knew that I had to have a hard drive to save everything on my laptop was I knew someone in one of these groups who invited me to a half day session talking about the risks, such as viruses, etc. And I learnt the solutions at that session. I would have never have known without that invite."*

> *"I went on a course once run by the WDA similar to that, a trailer that comes around and does a three hour session. That was very good, I learned a lot about security from that."*

> *"I phoned around and asked for recommendations... Word of mouth, sharing on forums, etc. will eventually mean the good products and services remain and the bad ones go."*

And within each group there was always a subset that knew 'someone who knows a lot about this sort of thing', who they turned to in order to ask questions when they needed an informed opinion.

[66] http://www.getsafeonline.org/

What emerges from all of this discussion, from the 'buyer beware' hard-line view, to those who experienced great value in the face-to-face awareness programmes, was that the onus is still on the individual to obtain the knowledge. It is acknowledged that the Government and private sector can put information in accessible locations but it is still down to the individual to seek out that information, take it in, and understand its relevance to their own situation. Attendee's comments show that negative experiences are viewed as a means to engaging with people:

> *"I think, it's like when you were a kid, and you mother said don't touch the oven because it's hot, you still touched the oven just to find out if it is hot, and it is only when you burnt your fingers that you then think that next time I won't."*

> *"A few people have to have the negative experience to teach the rest of the people what to do. It is like your analogy of taking bags to the bank. People are taking the bags to the bank, if enough people get robbed then everybody else will learn, don't do it."*

The data is not suggesting that *only* people who have had a bad experience online are capable of being aware of the risks and understanding the need to educate themselves. This relates back again to the value of face-to-face engagement with the issues of being safe online.

13.1 Comparing Our Findings with Other Data

As mentioned in section 2.2, alongside the data collected from the Trustguide workshops, our relationship with the Network Research Group, University of Plymouth has provided us with access to complementary data to compare with our own findings. In particular, a post-graduate project examining end user attitudes toward ICT security and their perceptions has allowed us to compare the survey data collected with the direction of our evidence.

The survey[67] was developed to measure end user attitudes toward security. It was disseminated virally, sourced from researcher personal contacts who were then asked to forward on to their contacts. As the survey wished to determine the perceptions of anyone who used the Internet at home, this dissemination method was entirely appropriate. The survey elicited 416 responses and the key findings of the survey are presented in Appendix A.4. The data provides a lot of supporting evidence regarding education in the Internet awareness arena.

The most telling figures we can draw from the survey focus around people's own skewed perceptions of their security awareness. This can be demonstrated through a number of responses; while less than 50% believe they are personally at risk from online fraud and over 60% believe that they have the requisite knowledge to protect themselves, when we examine their behaviour regarding how they protect themselves, the figures are more telling. When asked whether they understood the security features in a number of core applications used for online life, no more than 30% ever stated that they did. In addition, when examining update behaviour there are significant proportions of respondents who carry out updates no more than once a month. All of these figures show an imbalance between the users' perceived abilities and their actual behaviour. This is borne out a great deal in our discussions; we have many occurrences where individuals felt they were capable of protecting themselves, but perceived other, i.e. 'the public' to be in need of greater education and increased awareness. There is a theory attributed to media phenomena called the 'Third Person Effect Hypothesis'[68], that suggests that people believe they are less susceptible to the suggestive

[67] http://www.securityperceptions.net/

[68] W. Phillips Davis. "The Third-Person Effect in Communication", Public Opinion Quarterly, Vol. 47, No. 1 (Spring, 1983), pp. 1-15

nature of for example, TV violence, than other members of the public. We have significant evidence for this effect within our own work and it is also supported here. An interesting point is demonstrated by the final question on the survey, which examined whether there was any attitudinal adjustment toward their own beliefs regarding their capabilities for protection as a result of carrying out the survey. Only 13% stated they were more confident as a result of carrying out the survey. Significant proportions of respondents stated they were now more concerned, and wanted to find out more, etc.

This attitudinal shift is also interesting in the context of determining who the respondents feel is responsible for protecting them from the "perils" of online life. In the vast majority of cases, the individual felt they were the person most responsible. Initially, this may be viewed as being in contrast to our own discussions about who is responsible for protection, but when we consider the information sources that respondents turned to when wishing to obtain further advice, and where there is no dominant source, this might suggest that they feel they are responsible as they do not know who they can approach if they do not do it themselves.

This point leads us onto the final significant finding that supports our own work, that is, the ineffectual nature of mass media efforts to promote Internet awareness and safety. The awareness of Internet safety 'brands' is of concern in itself and unsurprisingly the BBC's efforts have more significant impact. However, what is more concerning is the perception of usefulness for those who are aware of the resources. There is strong evidence here to support our own data that suggests that face-to-face methods are far more effective than prescriptive mass media efforts.

13.2 Implications for Policy Makers and Educators

We recognise of course that Government is committed to making the UK the safest place to use the Internet (suggestions have already included PC and laptops being equipped with parental controls, new ways to fight against internet crime, and a child internet safety centre), all under the banner: "We will help protect consumers from the dangers of the 'darker side' of the digital world[69]." Backed by the police, charities and industry, the Home Office is in the process of setting up a multi-agency national Internet safety centre to deter criminals targeting the UK for Internet crime, and to reassure parents by exploring with industry how best to deal with 'unsuitable material,' use of parental controls, web blocking technologies and generally raising awareness on operating safely online. Government is also working with the banking industry to make that sector a market leader in terms of authentication. Obviously educators in these areas will come in many guises and we feel that our project has highlighted the issues they will face, whoever they may be. Not only do they have to convey the information in an accessible way, they also have to demonstrate the worth of the information to people who may not have enough experience to value it. However, what is clear is that human focussed techniques (mentoring, facilitation, 'lessons learned') are far more effective than mass media communication.

[69] March 2005 Connecting the UK: the Digital Strategy. Cabinet Office, Prime Minister's Strategy Unit, joint report with the Department of Trade and Industry.

14 School children and Internet Awareness

In the course of our adult discussion groups we came across several parents who were concerned about their children's Internet activity and their apparent lack of awareness that negative experiences could result:

> *"There are people who are scared of computers and worried about doing stuff but I look at my daughter using a computer, no fear whatsoever, do anything and she's eight."*

> *"That's the trouble I have with my kids, they're not frightened of what they download."*

As with the adult groups, what very quickly became apparent from the discussions with school children was that the different groups shared similar behaviours, experiences and opinions regarding online life.

What also became apparent is that the vast majority of attendees had considerable experience in using the Internet, in some cases going online was the primary means of communication with peers outside of the classroom. However, what was also very clear was that while there was considerable technical ability, the level of awareness and education around risk and threats online was less high. The following brings out key issues from the discussion and considers the implications of our dialogue.

The first aspect investigated in the discussion was the type of activities for which participants used the Internet. The vast majority of attendees had Internet access at home, used email, social networking sites (such as MySpace, Bebo, etc.) and Instant Messaging. This enabled a baseline for discussion, as we knew the participants had knowledge of the scenarios we wished to present to them.

The first aspect investigated was that of signing up to websites and being asked for personal details. The participants seemed very aware of the reasons for not always providing detailed information:

> *"I'm usually fine with it to be honest, but I tend not to sign up to them because I know that they are extremely annoying. Because you sign up and then they'll automatically piggy back onto your email account and email everyone in your address book virtually."*

> *"I tend not to upload photos or say actually where I am as well, because I think well, I'm just so wary of that."*

> *"Because a photo shows like your true identity, so you don't really want people, like if they come to Plymouth one day or something, they'll actually see who they've been talking to..."*

> *"There is always the opportunity that somebody is going to hack into it and get what little personal information you have put on there. But so long as you are careful about what you do put there, then there is nothing they can do with it."*

> *"Yeah. Everything else is fine, it's just the location."*

The majority were very clear that the biggest problems with personal information were addresses and photographs. They also had a number of interesting strategies to deal with these issues:

> *"Well yeah, I just, um, give a sort of vague idea, if they ask you where you live, just say um, Devon or something, and er, the alternative could be far from here, south west for example."*

> *"It's funny if you just type in false names that nobody is going to think of."*

"I've got a few different email addresses – I don't give out my personal one when I sign up to sites"

"I've put in false name and a false picture."

These quotes demonstrate a clear awareness of the potential issues in providing personal information online. When this awareness was investigated further, it was evident that participants had, in their own minds, clear understanding of where these threats might come from:

"I don't think it would make a difference, because as long as the people that go there aren't like pervs and that, then it doesn't matter."

"Because people can pretend to be you and like, if you get like benefits or something they can say we want them sent to like, this address and that, and then they get the benefit."

"You know I think the fact that you can choose exactly what you do put on there does give a level of reassurance, but you still think, well, you know, anyone could really view this on the Internet. And it still does worry me, yeah, when you see people's sites, you know, which have so much personal information on. You know, email address, phone number, photos of them and their family and all that stuff. It worries me that anyone can see that."

"When you think about it, how many girls get abused by paedophiles, or how many, you, know, the Internet is used for terrorists to meet, or you know, there are so many dangers to it."

In addition, attendees also showed an awareness of the traditional threats associated with Internet usage (malware, etc.):

"They might send you a virus, like it stays on your computer and they can see everything that's typed in. Even, if like the safety thing is on."

"Yeah, but if you get on those chain emails, there really annoying. Like there's one on MSN at the moment, saying 'send me a picture' or something, it would scan through all the viruses and if there was a virus, it wouldn't save it on to my computer or something."

"I had a virus once, but that was because somebody sent it to me through MSN."

The issue of countermeasures is an interesting one to explore; on the one hand the participants seemed very conversant with anti virus and firewalls as a means to block 'traditional' risks from the Internet:

"You've got like, usually, like on the computer you've got the Norton Antivirus and if you go on a dodgy site you know because it will pop up saying that it's blocked this website because it's got a virus on it, so you know not to go on it again."

"Well I use virus software called North32, I think this is brilliant. I've never had a problem since I've had it. It's really low pull on the memory, and it's really quick at scanning and it is better than the standard programs that you get. It's cheaper. It's an interesting program. Because I use Firefox, I obviously don't get the pop ups as well. So generally I don't seem to have too much of a problem."

Also, within the medium of Instant Messaging attendees were all very comfortable with blocking or removing people they did not wish to talk to:

"If you don't like the person you can block them, and you can delete them and…'

"Yeah, delete them…"

"I had some weirdo inviting me on MSN the other day, so I blocked them."

In addition, blocking was sometimes used as a social network management tool:

"Only people that I don't like, so if I've had an argument with my friends or something, I block them sometimes."

This, in particular, is interesting as it demonstrates quite clearly an example of a technology being used for something unintentional as far as developers are concerned. While blocking was built into IM applications to prevent people from getting in touch, did they consider it to be a form of social ostracism?

From the evidence presented above, we can show that today's teenagers are certainly technically capable in their Internet use, and have good awareness of threats and how to prevent them. They were also aware that sharing too much personal information can potentially be a risky thing to do. However, one of the most concerning aspects of our discussions was that while the participants had a good appreciation of the technical aspects of being online, and could speak with good awareness about the potential threats that being online posed, we encountered at least three examples of potential stalking:

"Every time I went on MSN, I found out she was very boring, so I didn't really talk to her and then 'Hello' how are you". Oh god. Block her. She was a complete stalker. 'Oh we could meet up sometime.' No."

"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 and stuff like this. He definitely was not, he was older; he looked so much older when he went on web cam. He looked really old. So then I just blocked him, I wouldn't let him, you know, he was asking me loads of weird questions and saying loads of stuff and I thought, that's not right."

"I went on MSN and my friend, he's like about 8 and I just went on to wish him happy birthday, because it was like his birthday coming up. I realised that it wasn't actually him I was talking to, so I got to his space on MSN, and he started swearing at me and this is like an 8 year old swearing at me. I knew him really well and he doesn't swear. So I just went, who is this, and he goes you should know who this is. I was like, but I don't. He goes, no, me neither. So I goes, like, ok."

However, in all these cases, while blocking excluded any further communication with the individual, the attendee describing the experience didn't think it was sufficiently serious to report to anyone other than their parents. There was never any thought to involve the police or service provider, etc.

In a number of ways, this apathy toward the online world, and its potential risks and infringements of privacy was demonstrated. In particular, threats to privacy such as mobile phone tracking and ID cards were not considered an issue:

When asked if they minded their parents being able to see where they are via their mobile phone many responded with:

"Why not."

"Yeah."

"Yeah! I like that."

> *"But then again, it could be seen as a good thing because you have a phone to tell them where you are anyway. So, it could be good, especially if you've got no credit or anything."*

Responses in respect to ID cards were similar:

> *"You get respect in different ways. You get more rights with an ID card. You get the right to vote and drink and that."*

Although some felt it was potentially a step too far in terms of parental intrusion into their lives:

> *"Yeah! I think that would work. You know, if you want to track my phone, well I want to track yours! Yeah, find out what your parents really do in their lunch hours..."*

In addition, in some of the groups we discovered that their school used fingerprinting to take books out of the library. Once again, there seemed to be little consideration for the potential infringement to privacy or civil rights this posed:

> *"Yeah, it's ok because you want a book."*
>
> *"Yeah, because the police could actually get your fingerprint up if they really needed it."*
>
> *"It's acceptable because the police can find you if you did something wrong, and there's fingerprints there, you can actually find out who's fingerprint it was, because it might be on the system."*
>
> *"It's only on the school records, so, it's only in school."*
>
> *"I think it would help in at least trying to identify criminals, or something. If you had all schoolchildren's fingerprints already on record. "*

We asked children how long the school kept their fingerprint records and found that most had not even considered this question and showed little concern:

> *"I think they keep them for a certain amount of time, a couple of years or something, but I've no idea. I think it's wiped off."*

We considered why this apathy existed. It seemed that none of the attendees were thinking beyond the immediate scenario or what they had been told from 'trusted' sources (i.e. their parents, their teachers, or the community policeman). They felt that they could not challenge this viewpoint, or present any alternative views. While beyond the scope of the Trustguide project, this does pose some interesting theories regarding the 'tipping point' where children move from being passive learners to actively challenging authority. We saw no evidence of this within our discussions so must conclude it comes, if at all, in later teenaged years.

14.1 Education and opinion forming

The issue of education is the crucial aspect to investigate with these particular groups of participants. We have presented a good deal of evidence regarding the level of awareness the participants had, but also the flaws in their views. We wanted to determine firstly where the participants had developed their knowledge regarding communicating online and the risks therein, and secondly what more they felt could be done. One of the most alarming aspects of this discussion was the lack of 'Internet awareness' taught in schools:

> *"It was like mainly at primary school when you had like lessons and people would say don't do this, do this."*
>
> *"The IT suite, you just got on with work really."*
>
> *"You get this set work that you do over a period of time."*

> *"You don't get any lessons about the Internet. It's just about work."*
>
> *"In school, like, one girl in primary school like done like computer crime and things, like to do with the Internet. Then you come here and you use computers, you can't help but pick it up."*
>
> *"But thing is it's not always right. So you don't know what to believe and what not to believe."*

It seemed that while some coverage of what is dangerous online was covered in some primary schools, secondary schools tended to follow an ICT syllabus but didn't consider Internet awareness or safety. Work carried out as part of a post-graduate project from the Network Research Group looking into issues of security awareness and education that backs up the claims of the group participants. Seven primary, and eight secondary schools were surveyed to determine the level of ICT security awareness addressed within their teaching. While all primary schools covered Internet awareness, only half of the secondary schools claimed this was covered. However, more concerning was that while half of secondary schools claimed to cover Internet safety, there was little promotion of resources such as Get Safe Online or Internet Safety Zone. Also, the majority of respondents felt that these topics weren't covered in sufficient depth.

Further analysis of GCSE and AS/A-level syllabuses also show a lack of awareness/social issues related to security. Syllabuses, understandably, focussed more upon core ICT practices and policies, etc. It would seem that awareness and protection of the individual in Internet scenarios falls outside of a traditional ICT syllabus.

Therefore, the children were left to look at other methods of developing their own understanding of the risks involved in going online. This appeared to comprise a mix of personal investigation, the media, peers and parents:

> *"It is common sense really isn't it? Or maybe you're looking for trouble if you give your address out."*
>
> *"I taught myself. Nobody else knows that I taught myself absolutely everything."*
>
> *"I did IT. I just picked it up."*
>
> *"You either learn or use common sense, you wouldn't like go out to paedophiles and give them your name and address and everything, so why do it on the Internet?"*
>
> *"Generally, the most publicised thing that I know about that happened is when MSN shut down its chat rooms. And that's years ago, yeah exactly, and that was the most publicised thing that I've known about really."*
>
> *"Yeah, I think I don't tend to watch TV much, but um, yeah, I mean there are all the safety type of adverts on the TV. I think AOL had their own one, and also you know the adverts for the Internet providers, and that was about how safe their particular services were, about the controls and things like that."*
>
> *"Because my mum works with like computers all day I would ask her before, just to check with it, because you know…"*

However, what is very apparent from both these quotations and observations from the groups is that the education regarding Internet awareness is fragmented and inconsistent. While some children felt that they could ask their parents, others had parents who were less informed:

> *"Yeah, my mum doesn't know anything. She doesn't even know how to turn the computer on. My Dad doesn't, my granddad does it the most but I don't see him a lot so…"*

This strand of discussion was developed to ask about participant's awareness of Government initiatives, such as Get Safe Online. Unfortunately, the level of awareness of the campaign was similar to that of adult attendees. The vast majority of participants had not seen anything of the campaign, and those who had had little recollection of its impact or message:

> *"The only one that I think that the government has ever done is I think about identity theft and that was really about hard copies, not the, you know, what happens in cyberspace."*
>
> *"I've seen an advert on TV. But it was only there for about two or three months and then it disappeared."*
>
> *"Well, I thought it was ok, because, you know your gonna be safe, like, you know nothing can really happen to you, really bad, at all. I think."*
>
> *"Boring.*
>
> *"Yeah, boring"*

Therefore, we asked attendees what they felt would be best method of getting the message across. This lead to much discussion around possible approaches and one of the most popular mediums was television:

> *"It's like all the soaps. I watch the Bill quite a lot, so it's all that kind of stuff is on there, like tracking and keeping safe and things like that."*
>
> *"You see things on the TV and you kind of like pick stuff up."*
>
> *"I think it would help, as well as a TV ad."*
>
> *"Stories have an impact. When you read like what happens, that can just be enough."*
>
> *"There was a programme about... it was on the gadget show, because it said about safe blockers and um, but a firewall and Firefox."*

However, the participants felt the most effective method would be within the schools. Schoolchildren already have special days as part of their "Citizenship" education for issues such as drugs awareness and bullying, and they felt that this would be the ideal forum for Internet awareness:

> *"I think what they could do is like an Internet awareness day where people came in like they do about drugs and things"*
>
> *"We could do it as part of Citizenship, we could do a day like we've done for drugs awareness"*
>
> *"It would work in school because you've got to go it then"*

In summary, our dialogue has demonstrated that among younger people there is undoubtedly a good level of technical ability; in some cases schoolchildren came across as more confidant than adult participants. They can also demonstrate good awareness of the potential risks and threats. However, what is more concerning is the 'patchiness' of this awareness, and the lack of activity in the event of a real threat. It is apparent that the awareness of schoolchildren is ill informed in places due, one would imagine, to the inconsistency in education of Internet awareness and risk. This issue is reflected in our discussion with adult participants; if the levels of education regarding awareness and Internet safety are insufficient, opinions are formed through positive and negative experiences, discussion with peers, and the media, etc. rather than reliable and genuine sources.

15 Guidelines

Sections 3 – 9 present data and discussion around the key findings from our work. In order to present this information in a manner that is usable by policy makers, educators, and service providers, we have taken core themes that have emerged from the considerable discussion to propose a number of guidelines that can inform the process of service engagement and delivery. The guidelines are presented in a discursive but structured manner; each guideline has discussion around key findings from Trustguide, followed by thoughts on how each could be achieved. All of the guidelines are supported strongly within the evidence presented in the preceding sections of this report.

TG.1: Education - Enabling better informed risk decision making

It is apparent from our research that education, in its broadest sense, is the fundamental foundation upon which opinion, and therefore engagement with online activities is formed. We have significant evidence that the entire risk/restitution equation, which results in either engagement or disengagement from an ICT mediated service, is built from the individual's belief system, which is informed by the sources of education available to them, as well as personal experience. Therefore, it is of considerable concern that the sources of education are so varied and incomplete.

If we initially take the adult perspective, it would seem that many participants felt that education was their responsibility, and there was a notable lack of support from what one might consider to be the key information providers – the Government and ICT service providers. While we must acknowledge that Government efforts exist (for example, the Get Safe Online campaign) the influence of these has not been significant. Awareness of the campaigns is fleeting and there seems to be little long-term impact. This promotional approach to using mass media has been demonstrated to be ineffective in other studies (for example, e-Gov engagement[70]). Drawing from the security percetions.net survey, awareness of the Get Safe Online 'brand' is approximately 11% of the population. The efforts, or lack of them, by service providers was also highlighted in our discussion – jargon heavy literature is off putting for the non-technical user. Therefore, people are left to their own devices to educate themselves from a number of, sometimes, non-authoritative sources. For example, popular media's influence in enabling people to form opinions has been highlighted, as have the potentially negative impact this can have. In addition, people rely on peers and their own experiences to build their knowledge regarding the issues of online life.

In considering the education of schoolchildren and the promotion of Internet awareness, the evidence is of even greater concern. While primary education does consider this is in a simple way, the development of awareness into secondary education is not present. At a time when children are becoming the most active online, and in some cases using the Internet as their primary means of communication away from their school, the education system is not providing them with a level of awareness that might help protect them. We have found, within our small sample, evidence of stalking on a number of occasions. While all of these experiences resulted in the blocking or deleting of the stalker, there was no evidence of an appreciation of the potential threat these activities posed. Once again, the users (in this case schoolchildren) are left to their own devices to educate themselves about the potential threats and again, this is generally a case of self-discovery and peer discussion. On rare occasions parents may be well enough informed to advise their child, but in a large number of

[70] Public Sector Forums (2006). 'Why Take-up Campaign Claims Are Complete Rubbish', http://www.publicsectorforums.co.uk/page.cfm?pageID=2641

discussions, the child felt either they, or one of their siblings, were more informed than their parents.

Therefore, we must conclude that a significant amount of effort still needs to be expended in order to better educate the population, and ensure a consistent level of knowledge. If we are to better engage the population with ICT based services, and reap the benefits this offers for both the service provider and consumer (i.e. better education leads to increased confidence, which leads to better and more informed decisions), we need a more consistent, engaging approach to the education of both children and adults.

There are a number of sources of evidence arising from our research that suggest directions for education. In considering the needs of the adult population first, we have evidence that awareness through mass media is ineffective, as is awareness that is viewed as being Government originated - it is viewed as being less authoritative as that coming from an independent source. However, in conflict with this, we also have evidence that people expect the Government to be the source of awareness promotion, as they are considered to be objective in the information they provide. In terms of effective engagement, there is evidence that face-to-face methods are a more effective means than mass media efforts. This is also borne out in other work looking at e-Government engagement[71]. Face-to-face approaches mean that the recipient is in a position to question the information provider and to build their own trust in the information with which they are being provided, i.e. the transfer of information is a two way process.

If we consider the technological adoption from a theoretical perspective, drawing from Diffusion of Innovations (DoI) theory[72], our findings are supported. Firstly, mass media is only effective in modifying weakly held beliefs; in understanding why people engage or fail to engage with online services, we are looking to a major attitudinal adjustment in their behaviour where there are issues of confidence, trust and knowledge. Therefore, it is difficult to determine how a mass medium could be successful in 'convincing' someone to change their behaviour and use something with which they have several barriers to overcome.

At the same time DoI theory puts great emphasis on *change agents;* individuals or groups that can play an active role in engaging with the new technology. These agents can come from numerous sources, but generally will have a trusted role with the target of diffusion (for example, a peer, trusted consultant, etc.). We have evidence of these change agents existing within our dialogue, for example participants have referred to learning from knowledgeable peers, and attending sessions from intermediaries such as Business Link, etc.

Therefore, while we can not demonstrate a conclusive, single method of education for the adult population that will work for the entire population, we can demonstrate that certain techniques are more effective than others, and that human to human communication, and the use of a trusted intermediary, are effective in promoting awareness that is long lasting and enables the recipient to incorporate into their own existing knowledge in an effective way.

For schoolchildren, we have a less complex problem in terms of technique as there is obviously an effective forum for awareness promotion – the child's school. Children also already have an accepted channel for awareness promotion in that they have drugs awareness days and similar as part of their citizenship curriculum and find it very acceptable to have a similar approach to Internet awareness. However, the method of dissemination is also important. We have good evidence that stories and case studies are far more effective than the presentation of facts alone. And again, the person to deliver the awareness is important; it

[71] "eGovernment Engagement Through Community Champions", A. Phippen, F. Land, A. Ward, Proceedings of eGov 06, Brunel University, September 2006.

[72] Rogers (1995). "Diffusion of Innovations (Fourth Edition)." Free Press. New York.

would be far more effective coming from a trusted source (e.g. a teacher or, in some of our cases, the community policeman), than an outside, unknown source.

Additionally, we have a different model for communication channels with children than exists for adults. Getting children online is not the problem, the online world is something that has always existed for them and they are comfortable with it. They have access at school and, for the majority of our sample, at home too. The problem is making them aware of the potential hazards about being online, whether these are fraudulent activity, malware, or potentially more dangerous personal risks (stalking, etc.). As children are comfortable with the web, and it is a medium they trust, it becomes an effective channel for awareness promotion. Many schoolchildren stated they had noticed adverts on MSN for example, and they could still recall the message when it had been presented in a strong image or story.

Finally, it would seem for children that television is a more trusted medium than it is for the adult population. We have evidence of awareness through television programmes being recalled by participants in our discussions that they described as effective, especially if the images were hard hitting and had a dramatic element to them. Again, factual presentation seems less effective.

In considering the 'how' element of this guideline, we have presented a number of methods that we can evidence as being considered effective in promoting awareness of online life and also some approaches that are less effective. However, it should be stated that while we can present evidence for some methods of dissemination as being more effective than others, there is clear evidence from our findings that there is also a need for further research in the engagement of ICT systems, how to promote awareness and how to educate a mass population.

TG.2: Experimentation – learning through doing

One of the key findings from Trustguide has been clear evidence that people do not believe absolute assurances that a technology is trustworthy and secure. Now that the Internet is an accepted part of major communication channels for citizens (i.e. TV, newspapers, etc.) even those who have no personal experience of use have strongly held opinions regarding the safety of online life. Therefore, providing unfounded assurances of security will not engage an individual with an online service in the first instance.

Individuals build trust with a service through experimentation. They will interact with a service that, in turn, enables them to build knowledge around its use. This ultimately leads to being able to make better-informed decisions regarding usefulness and convenience etc. We have shown considerable evidence of 'self discovery' from both adult and teenaged participants in the Trustguide discussion groups. Indeed, the majority of Internet awareness developed by teenagers seems to have come as a result of experimentation and discussion with peers. It is this experimentation that informs opinions not only of the service with which they are interacting, but also in building their own evidence base of online experiences in general. The extreme impact of a negative experience demonstrates this; if an individual has a negative experience online, it is unlikely they will simply cease to interact with a given service, they will cease to interact online.

However, with experimentation we should also express some caution. Without a sound educational process to underpin the experimentation process, opinions formed can be ill founded, especially if built upon already poorly formed knowledge. Therefore, one should view experimentation as a subset of education; in the same way we would not expect someone to learn how to drive by getting in a car without an instructor and 'play' with the machine until they discover how to make it work, we would not expect knowledge of online services to be built purely through experimentation.

When used to complement sound educational processes, experimentation can lead to strong relationships between the user and online services. Therefore, the facility to experiment with

an online service in a low risk environment (e.g. no financial transactions, no commitment to the submission of personal data) is crucial in achieving long-term engagement.

The experimental process should allow the user to discover the usefulness of the service and engage with their 'what's in it for me' assessment. They should have clear indications regarding how much of the 'real' service is available to them, and the anticipated increase in service provision outside of the experimental environment. This draws on a real world parallel with test-driving, 'try before you buy,' etc.

TG.3: Restitution Measures – provide a positive impact on personal perceived risk

Restitution is an important driver in the acceptance and adoption of ICT mediated services because such measures have a positive impact on perceived risk, are capable of restoring the last stable state before a transaction occurred, and circumvent the necessity to rely on confidence and experience built over long periods of usage.

Where restitution processes are in place this improves and encourages user confidence in entering into a transaction because the perceived personal risk with regard to the outcome is effectively reduced. We enter into transactions because we trust that our expectations will be met, (for example that goods will be delivered and will be of the expected quality), but if something goes wrong any risk can be mitigated by putting processes in place to ensure that there is no loss to the individual. Our findings show that in the case of commercial transactions over the web individuals enter into this arena with a greater degree of confidence than they might otherwise because any financial loss that may result is underwritten by a third party, namely their bank or credit card company. In such circumstances it could be argued that the perceived risk to the individual is reduced to the point of being negligible, that is not to say that risk is absent, rather the risk is shifted to a third party. Hence where risk is mitigated by restitution it relieves the degree of trust required to make a decision to enter into an ICT mediated transaction in the first place because some of the responsibility for a positive expected outcome is borne by a third party.

If something does go wrong and restitution can be made this has the effect of restoring the last stable state before the transaction occurred. In the case of commercial transactions in particular this ensures that is there is no financial loss to the individual. Restitution processes may take some time before any losses are reimbursed and of course cannot compensate for any resulting inconvenience to an individual. Hence it is not to say that restitution measures relieve the individual of the ultimate responsibility for making informed decisions, but they do improve confidence in the outcome.

The decisions we make about whether or not we can trust a particular vendor or service provider and the degree of confidence we have in those decisions are based on experience, either our own or that of people within our social circle whose opinions we trust. Building confidence takes times and increasingly in the fast-paced digital world we have to make decisions in less than ideal circumstances where the confidence we have in our decision-making abilities may be compromised. In circumstances where expectations are based on thin or even absent evidence (e.g. past experience, recommendations from friends) risk of loss, or of expectations not being met are perceived as high. The possibility of restitution being made underpins assurance that outcomes will be as expected or at least, if they are not, that any negative consequences will be minimised.

The potential of restitution being made is highly relevant to the degree of confidence users have in choosing to use ICT mediated services or make transactions and therefore lowers the barrier to use. Implementation of a restitution model is fundamental to the trust-confidence-increased-use process because it provides the basis of a satisfactory outcome. However sustainability of the current third-party restitution model, i.e. 'the bank will underwrite the cost to me if fraudulent activity can be proven,' depends on users ability to make informed

decisions as to whether or not they should enter into a particular transaction. We found many examples where attendees indulged in what they perceived to be risky transactions with a relatively cavalier attitude because they didn't perceive the risk to be their responsibility and were convinced their bank would underwrite any losses. Hence the role of effective education in this context cannot be over emphasised if we are to foster increasingly better-informed decision-making.

The key to successful restitution practice is to implement an easily comprehensible process that clearly spells out the phases of commitment, expected outcomes and fallback procedures in the event of any part of the sequence not being acceptable to either party. Restitution is of course far easier to achieve in some circumstances (e.g. financial loss) than others (e.g. stolen identity) as discussed in the body of this report. Where restitution cannot be made or is hampered by other complexities the scenario is quite different, and here the value of guarantees comes into play as will be shown in the following section.

TG.4: Guarantees – Provide assurance and improve confidence in whether to enter into a transaction

Hand in hand with restitution go guarantees. The age of innocence is over; across the board attendees repeatedly informed us that they believe it is impossible for electronic data to be held securely against increasingly innovative forms of attack. Our finding suggest that attempts to assure users that for example, certain services are secure are likely to be met with a high degree of scepticism. It is therefore at best inefficient and at worst dishonest to try to convince users that technology is entirely secure and trustworthy. Attendees were very aware that security is necessary but they were equally aware that it is not sufficient and a far more effective means of lowering barriers to use is the provision of guarantees.

Guarantees are important because they support the decision making process. A guarantee helps the user to interpret the degree of risk they are undertaking in an ICT mediated exchange, and what they can reasonably expect in terms of outcome. A guarantee also provides insight because it can be interpreted as a signal of intention that the vendor or service provider fully intends to fulfil their obligation and this supports the gathering of evidence that an expected outcome can be realised. Guarantees also provide rich cues for example, that a vendor or service provider is more worthy of trust than a provider that does not support their service with a guarantee, although to be effective of course, any guarantee must clearly state the extent of what is being guaranteed. It is equally important to state exactly what cannot be guaranteed in a transaction as well as what can be guaranteed.

The manner in which a guarantee is communicated and adhered to is also an important consideration, and above all, guarantees must be honest. For example, signifiers that a site is trustworthy are useful but attendees were highly aware that they could not always be trusted. They were aware that these signifiers vary in dependability according to context and location, that is, they can be copied or misused and hence are generally considered to be ineffectiveness and unreliable. Similarly the 'implied guarantee' that comes with complex technology is not well received, for example in the case of Chip & PIN the claimed trustworthiness of the technology is considered worthless compared with the restitution offered by the card issuers. This suggests that it is not the technology per se but the way in which it is managed and supported that impacts on acceptably, adoption and use.

It is also important to mention brand in this context because much of the value of brand lies in meeting and fulfilling consumers' expectations and this breeds brand loyalty and confidence. Brand loyalty is an invaluable asset because as far as the consumer is concerned it effectively acts as a guarantee of an expected outcome borne of experience over time, either first hand or second hand via trusted friends, family or other known consumers.

Guarantees then work in a similar way to restitution in that they offset perceived risks, help manage expectations, provide evidence and insight into the intention of a vendor and aid the

user in making better-informed decisions because they provide increased levels of confidence in the expected outcome being achieved. Where guarantees can be offered in conjunction with restitution processes any risk to the individual is considerably reduced, hence this serves to lower the barrier to use. Where restitution is not easily accomplished guarantees can provide similar assurances and it is vital that these are firm, honest and above all, adhered to with the highest levels of integrity.

TG.5: Control – Increased transparency brings increased confidence

Technology creates many new challenges and causes us to redefine that which we may have taken for granted in the physical world and one field where this is most apparent is the creation and protection of one of our most valued and most used attributes – identity. In its broadest definition identity includes all that information that is attributed to us as a unique identifier i.e. our personal data.

Attendees reported that as more data is gathered and stored electronically, particularly in centrally controlled databases, they feel more vulnerable. Much of this vulnerability is focused on a lack of control over who is collecting their data, who might have access to it, how their data may be used now or in the future and the potential for function creep. The problem is exacerbated by the fact that in response to perceived excessive requirements to provide more personal information than is deemed relevant to a particular interaction, and in order to wrest back some degree of control, users regularly supply false data. This combination of factors leads to an increased perception of risk in ICT mediated activities and highlights the importance of bringing confidence to these relationships. At the core of this of course is control of identity and personal data.

Users are clearly aware of the value of their personal information and certainly it should be gathered only with due and increased respect to individual rights of privacy and control. In the context of Trustguide we found that transparency about why data is being collected and how it will be used served to increase perceptions of confidence but this is of course dependent on the honesty and integrity of the data collector/holder/user. As we have reported, this in itself carries attendant vulnerabilities in that the people who have access to our data are considered the weakest link in the security of that information. Similarly it is important that required data to be entered in a given transaction should not be perceived to be excessive or inappropriate as this acts as a barrier to use since any data that is held electronically is widely perceived as potentially available to the public domain. Clearly spelled out statements as to how and why certain fields of information are required and how they will be used are vital ingredients in increasing user confidence, as are guarantees that are put in place to reinforce intentions of (restricted) specified usage. It is also increasingly clear that issues of ownership and use of personal data must be addressed and our research shows that the ability to access and manage data that is held about us would be welcomed because it improves transparency and therefore increases confidence. In practice this means providing users with the means to view, rectify and even remove information that is held about them, and this should be supplied in conjunction with providing stronger guarantees about how personal data will be used, stored and accessed. We recognise that it is difficult to provide guarantees across international boundaries, hence any UK legislation, in isolation, is unlikely support this endeavour. It is uncertainty that leads to lack of confidence and an increased sense of risk and it is these elements that we need to address more fully and competently.

If we are to design and develop trusted technologies we need to understand the complex inter-relationship between trust, confidence, control and security. The first issue that arises here is the need to understand that this is not simply a technological problem that can be solved in isolation by introducing increasingly strong identifiers and authentication processes. In order to address this challenge we must enter into a different arena, one that crosses the boundaries across different disciplines and traditionally this is an area where few have high levels of

expertise. If our goal is to develop technology that will overcome the barriers to acceptance, adoption and increased confident we must apply ourselves to this problem in a meaningful way and address it in combination with the social context and a deeper understanding of the attendant dependencies.

TG.6: Openness – honesty signifies and engenders trust

The final guideline underpins the different methods of engagement that exist within an informed information society (i.e. restitution, guarantees, control). Through effective communication of these methods, openness is achieved between the service provider and the service consumer. As stated above, the age of the innocent user is over – all current and potential consumers of a service perceive themselves to be informed to a greater or lesser degree. Whether their knowledge is accurate or not is of little concern in the engagement process, what is important is that the user believes they are informed and therefore enters into a transaction with a certain level of cynicism and scepticism.

We have clear evidence of this at various points in our discussion – the concept of a secure service, the guarantees offered by biometrics in being secure, ID cards as a means of reducing identity theft. In all of these cases people have dismissed claims of security, being told things in concrete terms without supporting these claims with evidence. Users are living in an age were they are constantly being informed about the risks of being online (however biased they may be). They will look for supporting evidence, alternative sources of information, etc. in building up their trust of a service and if these signifiers cannot be found, they will not engage.

A classic demonstration of the lack of openness, and therefore disengagement with a service, that was raised countless times within our discussions was that of terms and conditions statements. People believe them to be deliberately complex because the service provider does not actually wish for people to read them. We have observed many instances where people have not engaged with a service simply because they did not like the terms and conditions because they did not inform them effectively in their risk assessment process.

In achieving openness, we are faced with a mix of the methods discussed in the previous guidelines – openness can be achieved through education, experimentation, restitution and guarantees. All encourage openness through a variety of means, such as providing users with confidence to explore and learn, to appreciate and make more informed risk assessments, etc.

But most importantly, it is crucial that the service provider is honest and they do not make unsubstantiated claims of security, and do not provide guarantees that are untenable. Today's user is an informed, cynical individual; they cannot be bought with empty gestures. They need to be provided with the facilities to make their own judgements, and learn from their own mistakes.

16 Reflecting upon the Trustguide Experience

Our interim report (June 2006) represented work in progress and addressed some very challenging issues relating to public engagement and trust in ICT. Our final report has developed this work further, widening the geographical spread of participants and spending more time with educators and younger people, representing the next generation of service consumers. While the majority of this report is, quite rightly, focussed upon the presentation of evidence collected during our dialogue with UK citizens, and determining how this evidence can be best used to inform the development and policy making processes regarding ICT mediated services, it is also important to reflect on the process undertaken and where we might develop the findings of Trustguide further. While both Foresight and the Royal Society experienced problems in establishing an effective dialogue with citizens, one of our key successes was the level of engagement we achieved – approximately 300 UK citizens and 60 hours of transcribed discussion and it is therefore important to reflect upon the method and the learning opportunities this presented.

16.1 Evaluating our Method

As well as presenting the data collected from the project and discussing the implications therein, we feel that we are also engaged in a learning process with respect to the methods that can be used to research public engagement of ICT. We have already acknowledged the problems in establishing a dialogue with the public experienced by previous work, and feel there have been both successes and issues with the approaches used within Trustguide. As such, we will also be considering the lessons learned from our own methodological approach in order to inform any further research to be undertaken.

One of the most significant lessons learned from this work was how to initiate an opportunity for dialogue. There has been much discussion from the Foresight programme about the problems with engaging a population. We have certainly experienced similar in some instances within our own research. What is extremely apparent is that ‘cold calling’ and expecting people to want to attend workshops is unlikely to merit much success. Early recruitment attempts that were carried out via postal invitations and similar were not at all successful. Our greater successes in recruitment were through the value of viral dissemination and the exploitation of established, or known groups within the population. While the immediate concern with recruitment through personal contacts is the amount of bias in the sample that might result, the viral element that was included meant that while one or two key personnel might be known to one or more of the researchers, the majority were not.

The other area of greatest success was in carrying out workshops around a common profession/interest and this also benefited from a viral approach as attendees were keen to invite other people they knew who would also be interested in contributing. This, again, meant that a diverse group was achieved. And what is also clear from the presentation of our evidence is that while the groups may have been focussed around a specific demographic, profession, etc. the research design was effective in collecting their opinions, in the main, as private citizens. While interest specific discussion was used to establish a rapport with the audience, the research questions we needed to address were all folded into the discussion process. While this does require a skilled facilitator, and careful preparation and planning we feel our recruitment/engagement techniques are certainly transferable to other contexts.

We should also reflect on the use of technological engagement as a means of engaging participants in discussion. While, in some cases, the technological demonstration did elicit some discussion and get the audience thinking about privacy and security etc, we have little evidence to say that this was a strong method of engagement. There were a number of cases where technological demonstration was not possible, and in these cases we cannot report a less engaged audience than in those instances where technology was used.

There are several considerations to take into account in using cutting edge technology to engage attendees in the subjects under discussion, not least as representatives of HP and BT it was important not to give the impression that we were 'selling' our own products. In presenting some leading edge technologies, it was not immediately apparent to some attendees how this related to their own experiences of going online and we feel that engaging with existing technologies with which they were more familiar may have been as effective. In addition, due to the leading edge nature of some of the demonstrators, sometimes it did not work quite as well as expected and it is important to avoid negative experiences in this context. We also found that attendees could be equally engaged by focusing on current relevant news stories and provocative quotes from relevant documents on issues of security, privacy and trust that acted as a catalyst to discussion or helped to introduce new topics.

Finally, we greatly valued the benefit of a mixed methodological approach. While the core evidence for our work was drawn from focus group transcripts, non-verbal data and supporting surveys enabled us to greatly enhance the generalisability and validity of our approach. We are able to present our findings with greater confidence as a result of this supporting, complimentary data.

16.2 Dissemination plan

We recognise the need for a strong plan for sharing our results with others, in particular policy makers in central and local government, the EU and in industry and academia, who are the main recipients of our work. We have already identified many key individuals in roles where the findings of our report will have an impact and we will be distributing the final report to them. Also:

- We have had two papers accepted for publication in the BT Technology Journal [73] that have led to interested parties seeking us out for further information on the project.
- Hazel Lacohee and Piotr Cofta presented Trustguide as an exemplar of interdisciplinary research at the IOTR Systems and Services Science conference in Grenoble in September 2006
- Steve Crane had an article published in the IISP[74].
- Hazel Lacohee presented Trustguide at the BT Strategic Research Open Day on 29th June 2006 at BT Centre in London and both Steve Crane and Hazel Lacohee presented Trustguide at the second BT Strategic Research Open Day at Adastral Park, Ipswich on 12th July 2006.
- Steve Crane presented a paper at the IEEE SECURECOMM SeCoVal Conference in Baltimore, USA September 2006

[73] Phippen, A. & Lacohee, H. E-Government: Issues in Citizen Engagement. In press, BT Technology Journal, Special Open Edition, July 2006

Crane, S., Lacohee, H.,& Zaba, S. Trustguide: Trust in ICT. In press, BT Technology Journal, Special Edition covering HP-BT Alliance, October 2006.

[74] Crane, S. 2006. Trustguide: Trust in ICT. Institute of Information Security Professionals. http://www.instisp.com/index.htm

- Hazel Lacohee and Andy Phippen had a paper accepted for the Computers and Security Journal.[75]
- We are already influencing research within our own organisations. HP has started to research the impact of the guidelines on existing research projects, e.g. level of control considered acceptable by citizens trying to manage their personal privacy. BT has used the findings from Trustguide to support several major bid teams across the business and to provide supporting evidence for a White Paper on Identity. These activities within BT and HP are ongoing and will continue to be developed.
- Interest in the findings and potential impact of the project grew after we exhibited at the InfoSecurity event in April 2006, where we supported the DTI on their stand by providing information about the project to visitors.
- Further public awareness of the project was achieved through our contribution to the Cabinet Office CSIA (Central Sponsor for Information Assurance) Road Show that recently toured the UK[76].
- Hazel Lacohee presented Trustguide to Unilver in October 2006.
- Trustguide was featured in the BT Collaborative Research Newsletter in October 2006.
- We have submitted a response from the project to the call for evidence from the House of Lords Science and Technology Committee to investigate personal Internet security[77].
- Trustguide results will be exhibited at the 18th HP Security Colloquium at Royal Holloway, 18th December 2006. This highly recognised 'by invitation only' event attracts 120+ leading information security experts including CIOs and Head's of Security from across the UK and globally.

16.3 Developing Trustguide

We believe that one of the most significant findings of Trustguide was clear evidence for the concept of the ‘informed user’, regardless of their technical experience. The implications for these results are far reaching, potentially changing methods for developing security into ICT mediated services, considering how policy informs the public engagement of ICT and how service providers engage new users. In particular, we feel the following are crucial in developing an effective relationship between the general public and ICT mediated services:

- Education and awareness – how policy makers and service providers can best educate potential users in order that they make informed decisions, rather than the general approach of building knowledge on poor foundations based upon peer discussion and mass media potentially biased reporting.

[75] Lacohee, H., Phippen, A. & Furnell S. 2006 Risk and Restitution: Assessing how users establish online trust.
http://www.sciencedirect.com/science?_ob=HomePageURL&_method=userHomePage&_btn=Y&_acct=C000061901&_version=1&_urlVersion=0&_userid=3962339&md5=e538210f56aefac106bde13922b1cf81

[76] http://www.kablenet.com/events

[77] http://www.parliament.uk/parliamentary_committees/lords_s_t_select/internet.cfm

- Protection of the young – one area of most concern arising from the findings of the project is the failure of the education system in promoting Internet awareness and protecting the young from the potential threats of cyber stalking, bullying, etc.
- Understanding the trust/risk/restitution model – we have identified a far more complex model of engagement than that which is presently understood within the service provision sector. If engagement is to be effectively achieved, far more work needs to go into understanding this model and disseminating to service providers.
- Interdisciplinary research - what is also key within the development of work in the field of trust and engagement is the need for *interdisciplinary* research, something that was immediately apparent when considering the authors' own perspectives (psychological, technological and socio-technical) and this point is developed and demonstrated in the following section.

17 Conclusion

The question remains as to whether there can ever be a consensus regarding what is reliable and trustworthy. Understanding that the word 'trust' is overloaded with meanings suggests that this is unlikely. However, our research reveals that what people want when they call for trust is a perception of confidence; the mix of secured control and trust that will help them to develop their ICT mediated relationships. Mobile technologies, pervasive computing, broadband etc. bring many challenges not only to managing security or reliability as such, but first and foremost, to the perception of how trustworthy a system actually is. 'Doing security properly' in order to enhance trust and privacy concerns is simply no longer sufficient.

However, security and trust are intrinsically intertwined, and this goes well beyond what the ICT security community is willing to admit; security is built on trust and trust is built on security. People are the weakest link in security systems but they are also the last resort if such systems are compromised; they are both the reason to exist and the limiting factor. Neither technology nor social sciences can describe or resolve the problem alone. Hence we feel there is a strong and urgent need to combine multiple methods for research and development across multiple disciplines and from different perspectives including users, designers, developers and hackers, and this raises another difficult question, that of how this might be best achieved.

These problems will require constant and meticulous research if we are to achieve Government's vision of everyone in our country confidently enjoying the benefits that increased use of ICT can undoubtedly bring. We need to understand the issues of today and those that may arise in the near and more distant future. Security cannot be treated as a separate or distinct issue from trust given that it is intrinsically linked to the issues that impact on adoption, acceptance and confidant use of both new and existing technologies.

We can drive adoption and improve people's perception by giving them reasons to trust technical systems but this must go beyond the blind trust that is offered today. People are sceptical about technology, and rightfully so. However, if empowered and allowed to experiment, they tend to adopt solutions that are socially beneficial. The changeover will not happen overnight, but it should be driven by people's ability to correctly ascertain the extent of trust they can extend towards technology. Secure experimentation should allow users to gather positive experience and open the path to an improved relationship. Education of course is also essential in creating the mindset that is both inquisitive and understanding.

Trust is a construct that calls for interdisciplinary research. However, reviews[78] confirm that there is a significant rift between research in trust within the context of social sciences and the context of computer sciences. Social sciences interpret trust as a relationship that can develop between two or more human beings while computer sciences are mostly interested in 'security and trust' management between computers. We feel that a fruitful way forward to ensure that we are addressing the most relevant and appropriate research questions is to draw together a community of people from different backgrounds and disciplines to work on this together so that we can employ different sources of expertise including security, community, and social scientists.

Below we describe one example of how an interdisciplinary approach to the issues of trust and security can come to very similar conclusions from very different perspectives and the value that each approach can bring to the other in terms of enhancing our understanding and making our findings accessible and relevant to both practitioners and policy makers. While we employed qualitative social science research techniques within the Trustguide project,

[78] e.g. Abdul-Rahman, 2005, op cit

work with a similar focus was being undertaken by Piotr Cofta[79] from the perspective of building a theoretical model of trust. His theoretical research has concentrated on trust in and through the interplay between society and technology, looking at the unification of disparate concepts of sociological and technical trust. It has eventually led to the formulation of a concept of Trust Enhancing Technologies (TET); the identification of a set of five core technology properties that should facilitate the creation and retention of trust in a digital environment.

Through the iterative and interdisciplinary approach, not only has the concept of TET allowed us to structure the discussion within Trustguide, but also Trustguide was able to deliver strong evidentiary support for the majority of TET's proposed properties. The demonstrated value of such interdisciplinary cooperation opens up new opportunities to unite social and technical perspectives on trust for the benefit of individuals and society more generally.

We have presented compelling evidence that challenges current thinking on how to engage citizens with ICT mediated services. Whilst at the inception of the project we might have expected to be able to develop a number of clearly measurable principles that could be adopted by a service provider and 'dropped in' to their development processes, our results show a far more complex relationship that demands further in depth research. We have revealed a relationship between an informed user and service provider based upon trustworthy information, control, confidence, informed risk analysis, guarantees and restitution measures, and perceived individual benefits. We have also suggested the need for a different focus that is, quantifying risk rather than building stronger security measures in isolation from the social factors that impact on technology acceptability. Further, it is clear that education and assurance underpin confident use and informed decision making in ICT use and it is evident that current education measures are failing both the teenaged and adult populations, which results in knowledge being built upon unsteady foundations and this should be addressed as a matter of urgency since it is clear that negative experiences generate barriers to further use.

If our goal is to develop technology that will overcome the barriers to acceptance, adoption and increased confident use we must apply ourselves to this problem in a meaningful way and address research in combination with the deeper social context and a broader understanding of the attendant dependencies.

[79] Piotr Cofta, 2006: Trust Enhancing Technologies. In: Trust and control: confidence for the convergent communication (in prep.)

A.1 Appendix: Example technology demonstration and discussion format

Trustguide workshop 10 May 2006

Mobile II: Peer-to-peer

Demonstrators: Kenton O'Hara and Tim Kindberg, HP Labs

A.1.1 Demonstration Overview

Explore trust-related issues for peer-to-peer interactions over short-range wireless – principally Bluetooth. Investigate participants' attitudes to and knowledge of trust-related issues, and how they vary by place and application. In particular, look at the type of content being transferred (which may differ in how private it is considered to be), and whether the (apparent) source is known.

A.1.2 Introduction – background and workshop aims

Organisers give overview of workshop.

Participant introductions. Have they ever used Bluetooth, infrared or SMS for a local interaction with another person or perhaps with a laptop or other machine?

A.1.3 Exercises

Each pair of participants will get a phone and try the following exercises:

Each phone will have (a) a name set by us; (b) a few images chosen and installed by us.

Exercise A. Discovery

We ask participants to look at which discoverable Bluetooth devices are around. We'll have chosen the names in the area to range from bland (e.g. Nokia 3650) to more personalized

We then ask them to choose & set their own phone labels, and do discovery again.

We ask a few questions at the time, such as: what do you think of these names? Do you have any idea whose name is whose?

[If there is time: we get them to investigate the range of Bluetooth. How far before a particular phone is no longer discovered?]

Exercise B. Exchanging content

Each phone has three images: landscape, child, humorous cartoon

(In pairs of phones:) Each sends the same landscape image to the other phone, which requires communicating their respective phone names and doing discovery.

We ask them to consider whether they would send the child or humorous cartoon, assuming they had chosen it themselves.

Exercise C. Receipt of unsolicited content

We use two phones, one called "HP Labs", the other called "jimmyJonz" (or some such) to send a pair of files to each phone: an advertisement for HP printers, and a file called 'caribe.sis' (which is the name of an actual worm but we won't use that file itself!). "HP Labs" will send both, "jimmyJonz" will send only caribe.sis. It won't be obvious who is sending it.

A.1.4 Discussion

In relation to the technology demonstrated:

Attacks – do they fear attacks against the integrity or privacy of their personal data, the phone's ability to function, or …

Place – how would different environments affect their willingness to engage in applications such as they have seen – e.g. the street versus the pub versus a café versus your home.

Personal identity projection – what would the participants feel comfortable with projecting about themselves to others from the phone, including and beyond the name they use? What do they feel about others' identities being projected through the names they use, and perhaps more?

Applications – how would their attitudes vary between applications such as a game, music sharing or chat?

Unsolicited content – what do they feel about unsolicited commercial content, such as sound clips from music posters? – How about unknown files such as the one we sent to them?

What would reassure them? – against the attacks they identified?

Followed by the semi-structured professionally facilitated discussion.

A.2 Appendix: Example of analysis using QSR N6

QSR N6 Full version, revision 6.0.

Licensee: Andy Phippen.

PROJECT: Trustguide, User Andy Phippen, 8:46 am, Jun 13, 2006.

REPORT ON NODES FROM Tree Nodes '~/'

Depth: ALL

Restriction on coding data: NONE

(1) /Engagement

(1 1) /Engagement/methods

(1 2) /Engagement/attitudes

(1 3) /Engagement/audience

(1 4) /Engagement/of technology

(2) /Technology

(2 1) /Technology/Authentication

(2 1 1) /Technology/Authentication/positive experience

(2 1 2) /Technology/Authentication/negative experience

(2 2) /Technology/Biometrics

(2 2 1) /Technology/Biometrics/positive experience

(2 2 2) /Technology/Biometrics/negative experience

(2 3) /Technology/Proof of identity

(2 3 1) /Technology/Proof of identity/positive experience

(2 3 2) /Technology/Proof of identity/negative experience

(2 4) /Technology/Trusted third party

(2 4 1) /Technology/Trusted third party/positive experience

(2 4 2) /Technology/Trusted third party/negative experience

(2 5) /Technology/eGov

(2 5 1) /Technology/eGov/positive experience

(2 5 2) /Technology/eGov/negative experience

(2 6) /Technology/updates

(2 7) /Technology/ID Cards

(2 8) /Technology/eCommerce

(2 8 1) /Technology/eCommerce/positive experience

(2 8 2) /Technology/eCommerce/negative experience

(3) /Awareness

(3 1) /Awareness/of threats

(3 2) /Awareness/of risks

(3 3) /Awareness/of crime

(3 4) /Awareness/of anonymity
(3 5) /Awareness/of non-repudiation
(3 6) /Awareness/of technology
(3 7) /Awareness/of online environment
(4) /Responsibility
(4 1) /Responsibility/Facilitation of security
(4 2) /Responsibility/for protection
(4 3) /Responsibility/for education
(4 4) /Responsibility/for legislation
(4 5) /Responsibility/for control
(5) /Online behaviour
(5 1) /Online behaviour/eCommerce
(5 2) /Online behaviour/Banking
(5 3) /Online behaviour/Searching
(5 4) /Online behaviour/Browsing
(5 5) /Online behaviour/Email
(6) /Problems with technology
(6 1) /Problems with technology/security
(6 2) /Problems with technology/connectedness
(6 3) /Problems with technology/usability
(6 4) /Problems with technology/functionality
(A) //Document Annotations
(F) //Free Nodes
(F 1) //Free Nodes/Education
(F 2) //Free Nodes/Offline behaviour
(F 3) //Free Nodes/Impact of the Internet

A.3 Appendix: Schools Method

Pre-group Questionnaire

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

1. Please list below how you make use of the Internet.

2. Do you use Instant Messaging?
   Yes No
3. Do you use a blog?
   Yes No

   If yes, which one?

4. Do you use the Internet frequently to communicate with your friends?
   Yes No

5. 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.

6. Are you worried in any way about how much personal information you have given to these websites?
   Yes No

Questions:

Please consider the following scenarios:

2. 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.

    1. What do you think about when answering these questions?

    2. Do you mind giving the answers?

    3. Does it worry you to give out this information?

    4. Do you remember what you've said and where?

3. This website that you have signed up to allows friends of your friends to see your details.

    1. Does this worry you?

    2. How might you control who sees or finds out what about you?

    3. Do you feel you are in control of your personal information?

    4. Do you feel that technology affects how you control your personal information?

    5. For example, do the new features on your mobile phone affect you?

    6. 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?

    2. If you have, what are your thoughts on them?

A.4 Appendix: Key findings of security perceptions.net survey

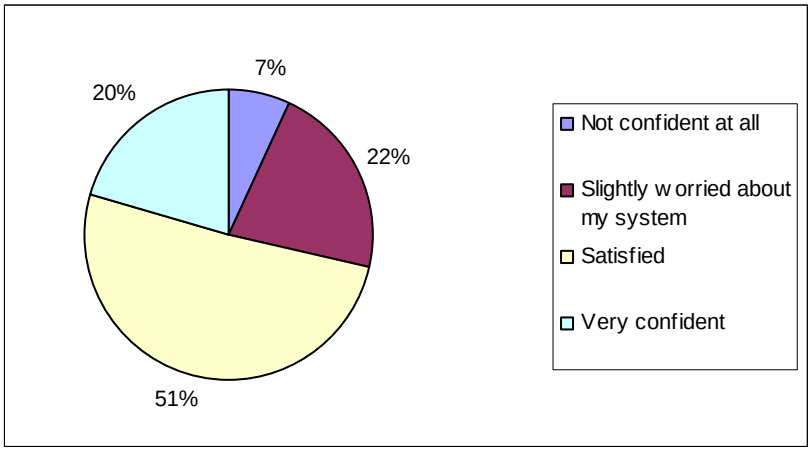

Figure 2: Respondents' confidence in the security of their system

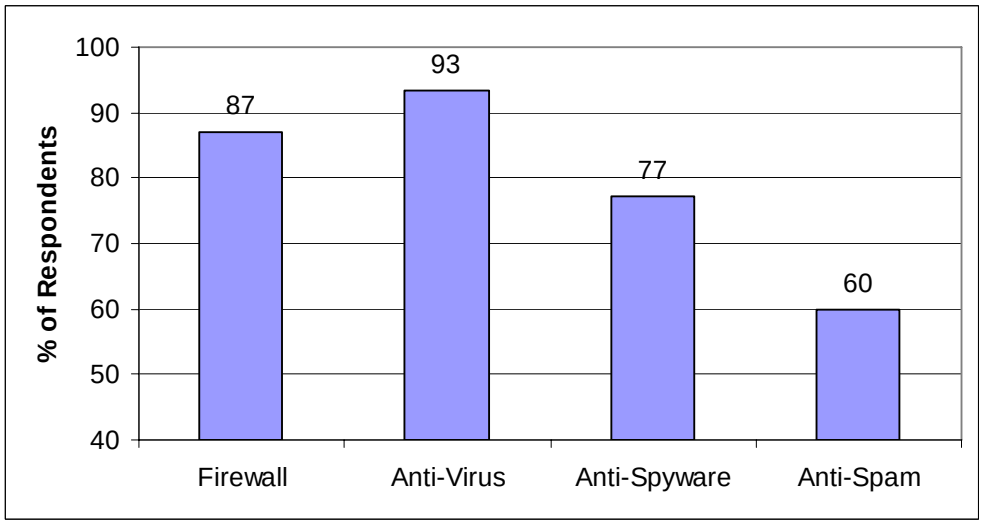

Figure 3: What security technologies do respondents have in place installed on their machines

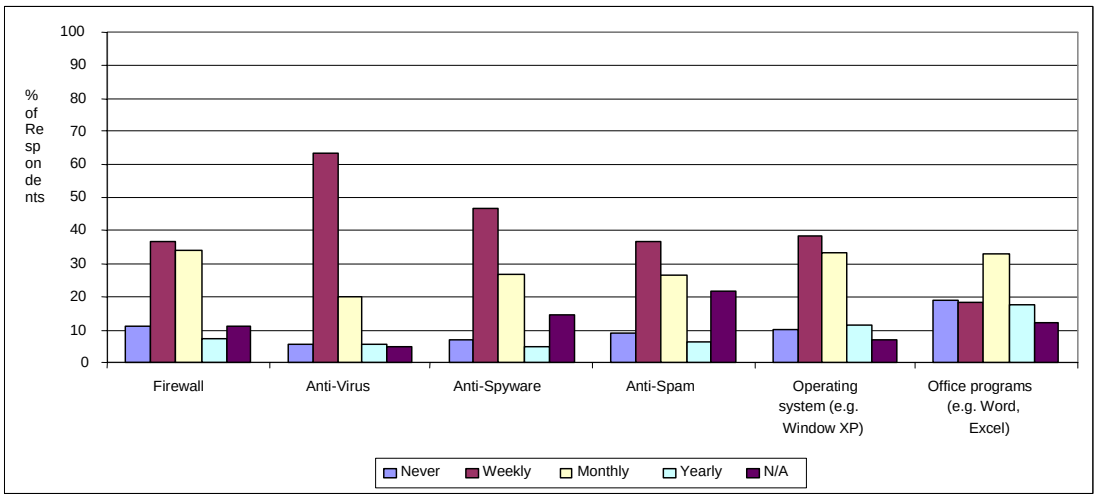

Figure 4: How often do users update applications

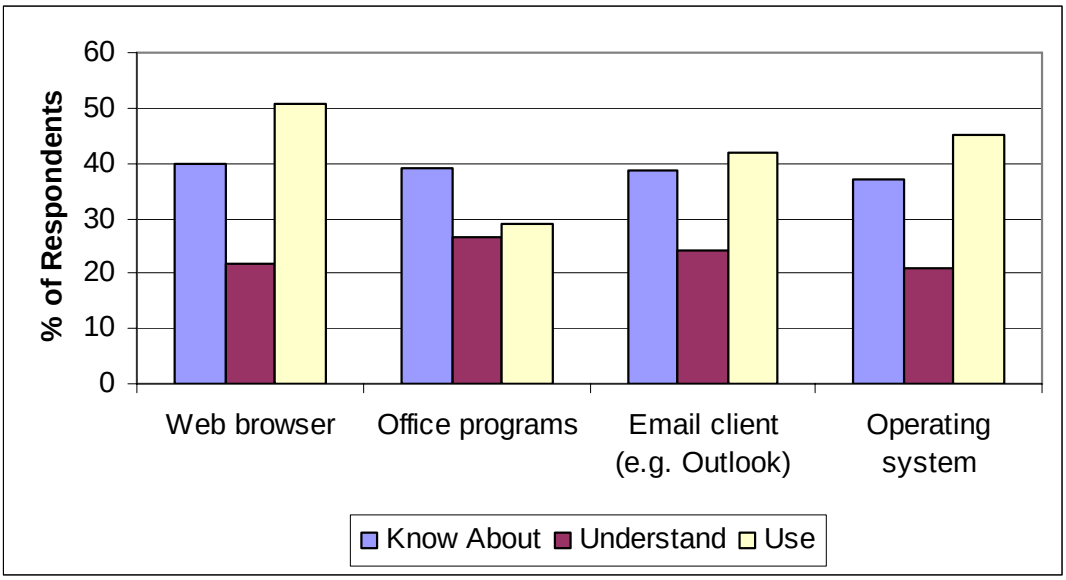

Figure 5: Users experience of security features within programs

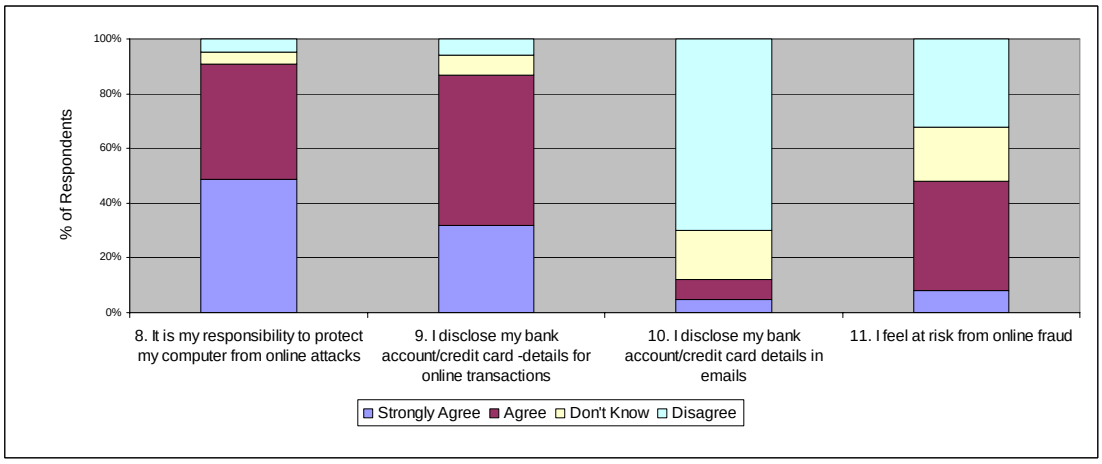

Figure 6: Attitudinal measures regarding sensitive issues

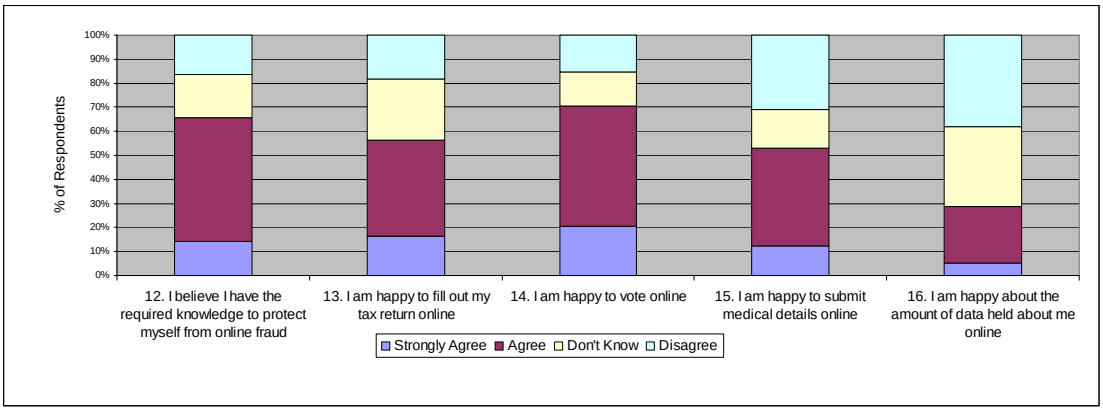

Figure 7: Further attitudinal measures regarding sensitive issues

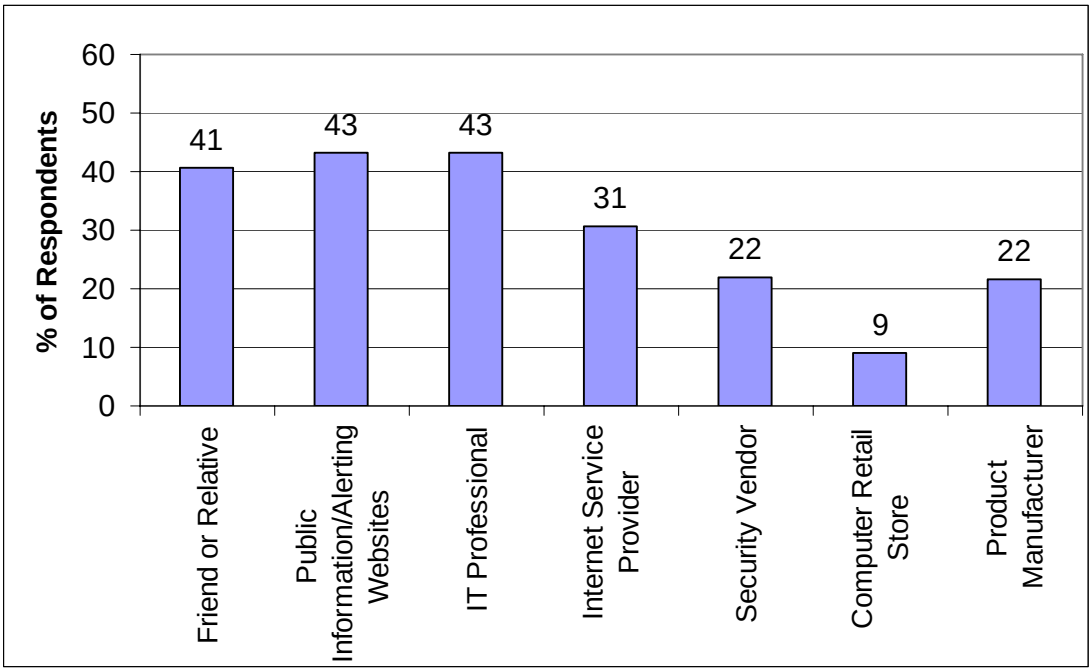

Figure 8: Sources of knowledge for education and awareness

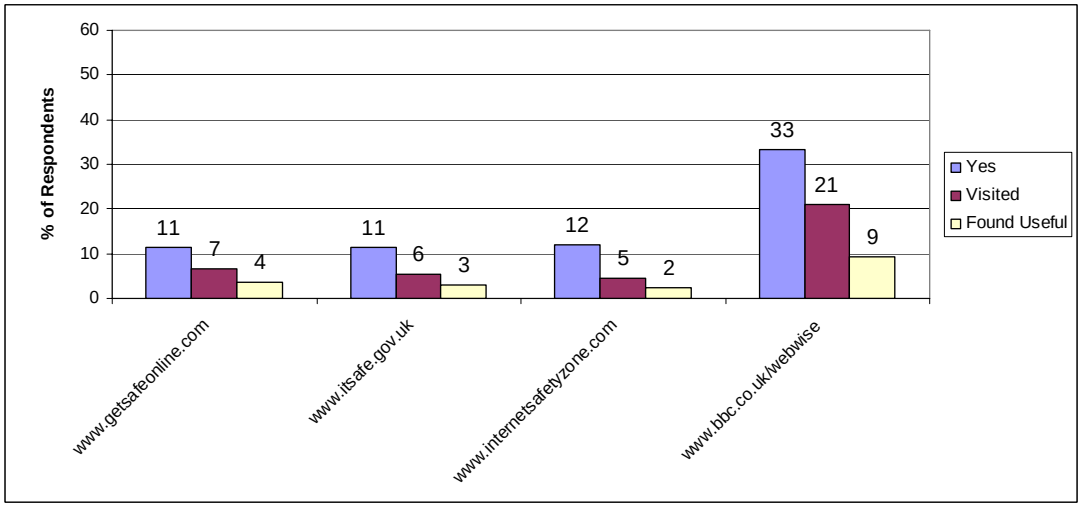

Figure 9: Awareness of national initiative on online safety

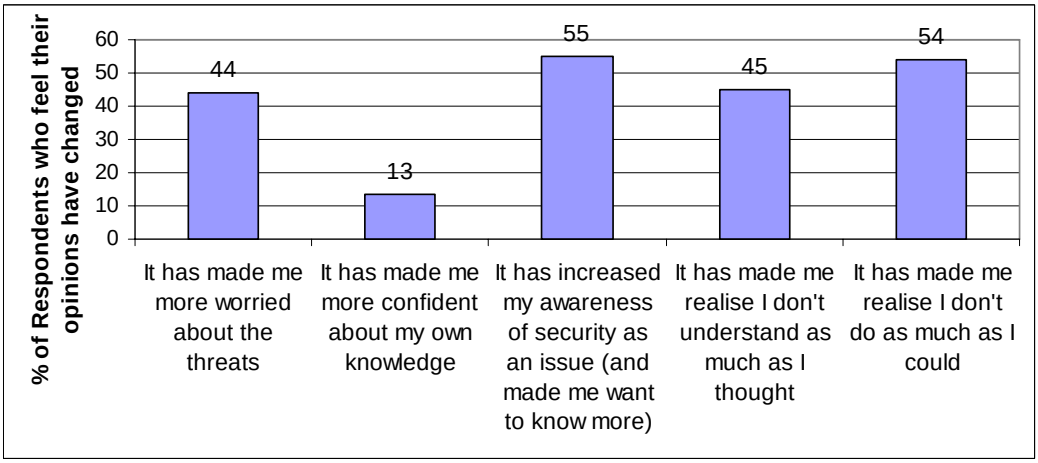

Figure 10: Feelings having carried out the survey