

Building a Culture of Trust in an Online World: A Citizen-Centric Approach

Dr Hazel Lacohee, BT Group Chief Technology Office, Research & Venturing

hazel.v.lacohee@bt.com

ABSTRACT

Our research 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 covered as broad and appropriate a spectrum of the UK's citizens as the scope of the project allowed. We took a citizen-centric approach with the aim of using 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.

If, as a society, we are to take full advantage of the transformative power of ICT we must ensure that we build a population of confident, informed users who are aware of and understand the attendant risks and responsibilities. The principle issue that arises from our research is the need to understand that this is not simply a technological problem that can be solved in isolation; in order to address this challenge we must enter into a different arena, one that crosses the boundaries between different disciplines. Citizens are sceptical of claims of security in relation to ICT, and rightfully so. Our findings suggest that it is not trust per se that should be 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. While legislative measures have their role to play in helping to protect consumers, this is not sufficient; education and assurance are the foundation of confident use of online services and emerging technologies that will fulfil the vision of an ICT-enabled future. If our goal is to develop technologies that will overcome the barriers to acceptance, adoption and increased confident use we must apply ourselves to this problem in a meaningful way, addressing the technological issues in combination with the deeper social context and a broader understanding of the attendant dependencies.

Introduction

This paper draws on the findings of the Trustguide¹ project that was designed to build on the findings of the UK Department of Trade and Industry led Foresight Cyber Trust and Crime Prevention Project². Trustguide was a collaborative project between BT Group Chief Technology Office Research and Venturing and HP Labs and was undertaken with support from the University of Plymouth's Network Research Group³.

The UK Government wants the UK to take full advantage of the opportunities offered by scientific discovery and technological development and aims to build societal

¹ <http://www.trustguide.org.uk/>

² http://www.foresight.gov.uk/previous_projects/cyber_trust_and_crime_prevention/index.html

³ University of Plymouth's Network Research Group, <http://www.network-research-group.org/>

confidence in the decisions that are made in the development, governance, regulation and use 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. In order to do this we need to understand the deeper social context and the attendant risks and benefits for the development and delivery of trustworthy ICT, and equally how to build a population of confident and informed users.

We took a "citizen-centric" approach to exploring issues of trust, security and privacy in order to better understand the reasons behind how and why UK citizens engage with particular ICT based applications and services. We conducted our research via a series of 29 workshops and discussion groups involving in-depth dialogue between September 2005 and October 2006 that covered as broad and appropriate a spectrum of the UK's citizens as the scope of the project allowed.

The key objectives of the Trustguide project were:

- To build on the outputs of the Foresight project
- To 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
- To produce guidelines for those engaged in the research, development and delivery of ICT on how cyber trust might be enhanced

We employed a focus group based methodology where small groups of citizens entered into discussion around issues concerning the following topic areas:

- Data collection: trust, risk, and responsibility
- Authentication: Chip and PIN, ID cards, use of biometric data
- Identity: theft, privacy and fraud
- Achieving successful ICT engagement with the public
- Public Sector IT and e-Engagement
- Acceptability of public surveillance
- The human element in security: the weakest link
- Awareness and education
- Enhancing privacy: third party management and legislation
- Public access terminals; mobility and location based services

The groups were drawn from different sectors (for example, SME representatives, students, ICT service developers, user groups such as farmers, as well as the general public) and from a number of geographical locations in the UK in order to ensure as wide a coverage of opinion as possible. We also included 'novice' and 'expert' groups (for example corporates, academics and researchers engaged in this area) as we envisaged that we would be able to compare and contrast opinions across groups according to differing levels of ICT awareness and expertise. In addition to this we

also carried out discussions with a number of groups of schoolchildren in order to assess the opinions of the next generation of ICT service consumers and producers who are already part of the online audience and are already targeted by service providers.

The discussion groups were professionally facilitated and observed by at least one other researcher and in all cases attendees were asked to express personal opinion, and experience rather than company policy. Discussions were recorded, transcribed, and analysed for common trends and themes and we used the results of 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.

What do we mean by trust?

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. But 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 agree⁴; 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 trust is a personal characteristic based on choice (to trust or not to trust), more generally social science defines trust as ‘an attitude of positive expectation that one’s vulnerabilities will not be exploited,⁵’ and dictionary definitions include ‘...a firm belief in the reliability or truth or strength etc. of a person or thing...a confident expectation...and reliance on the truth of a statement etc. without examination.’ Trust is only necessary of course where there is something of value that could potentially be lost. 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 and this is of even greater importance in an ICT mediated environment where none of the cues that are available in face-to-face transactions, and upon which we partly base our trust decisions, are available. Throughout our work we have taken a simple operational definition that interprets trust as an individual belief. However it is important to point out that even this simplified definition entails further consideration because beliefs influence actions. In fact trust rarely operates in isolation from other beliefs and influences and although it emerged from our discussions that UK citizens do not trust technology, this does not inhibit use of the many ICT mediated services available, in fact quite the contrary.

“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.”

⁴ 2001 D. Harrison McKnight & Norman L. Chervany. Conceptualizing Trust: A Typology and E-commerce Customer Relationship Model.

⁵ 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

“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.”

Our research suggests that it is not trust per se that should be 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. Not that this makes the task in hand any easier; the concept of what constitutes a risk, and under what circumstances, is probably open to as many definitions and interpretations as the concept of trust. However, it is interesting to note that attendees more commonly referred to ‘risk’ than ‘trust’ when describing their ICT mediated experiences and it is management of these perceived risks that are worthy of a good deal more attention:

“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.”

“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.”

While there are a number of different issues presented within the Trustguide Report as described above, there is one cross cutting theme that emerges; people are sceptical about technology and rightfully so. 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 have something to gain, are informed about the possible outcomes, and it is clear how consequences will be addressed if the expected outcome is not met. 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, guarantees are in place and restitution will be made.

Key Findings

Our findings suggest that UK citizens are technology aware and have belief systems informed by a mix of mass media communication, personal, and peer experiences. But what is important to remember is that whether or not one agrees with the views and opinions expressed in the body of this paper, or indeed within the Trustguide Report, and whether or not one considers those views to be correct, this is what our sample of UK citizens held to be true and it those views and opinions with which we must work if we are to better understand how we can build a culture of trust in an online world.

One of our primary findings was that people were concerned about their personal data being held electronically and across the board. Whether part of our ‘expert’ or ‘novice’ groups we found that people were highly sceptical about claims that electronic data can ever be held securely. The age of innocence is truly over – we found an intense distrust of electronic data gathering, storage, amalgamation of databases and the potential for function creep. Of particular significance in relation to

government and the use of e-gov services we found a general distrust of government's ability to hold data securely; for example very few attendees felt that the introduction of ID cards would aid either their personal or the nation's security and hence could not perceive any advantage. However concerns were mainly centred on Government's ability to hold ID data securely because of the high appeal of such information to hackers and this highlights the flip side of advantage - that of the potential impact of loss and how in turn this influences belief and hence behaviour:

"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."

Certainly the high profile reporting of UK Government's ability to deal with large IT projects in the mass media have contributed to both government's reputation in this respect and the mistrusting nature of the citizen. But the comment above is perhaps the most enlightening because we found that guarantees and restitution measures were far higher on the agenda for most people than claims of security. If something should go amiss the most important issue for people is the ability to guarantee restoration of the last stable state, and minimise any personal inconvenience and/or cost and this is critical to adoption in the ICT mediated environment.

Building a culture of trust

Users do not enter into an online engagement because they believe it to be secure, they do so because there is some benefit to be gained and any potential loss can be mitigated. In considering engagement with an online service, they carry out a personal risk assessment and balance this with the potential benefits, albeit with varying degrees of competence. In carrying out this risk assessment users are more likely to engage with an online service if it is clear what the potential failings could be, and how the service will rectify any emergent problems. Clearly guarantees of apparent security and one hundred percent secure, 'unhackable' technologies will be met with a high degree of scepticism but where claims of security fail, restitution measures and guarantees of an expected outcome are extremely robust, positive indicators of acceptability and adoption.

There are, however, a number of other issues that influence trust in an online environment. 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. 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."

Decisions based on reputation of a given company may rest on first-hand experience or that of trusted friends, relatives or media reports. While it can take a good deal of time to build a reputation of trustworthiness it is a fragile phenomenon that can be easily broken by a single bad experience or adverse reporting in the media.

“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.”

Education is also fundamental to the decision-making, opinion forming and risk analysis process; potential users who are well-informed are more likely to confidently engage with ICT mediated services than those whose knowledge is built on shaky foundations. Our research showed that in this respect education is failing both in the adult world and amongst schoolchildren and there is a clear need to address this as a matter of urgency:

“If we educate ourselves, if the government makes it a priority to educate people, then we won’t fall foul quite so much.”

“You don’t get any lessons about the Internet at school. It’s just about work.

Our observations reveal that currently education regarding Internet awareness is fragmented and inconsistent and clearly this impacts on the ability to make informed decisions regarding potential risks. Allied to education and increased confidence is the ability to experiment in a risk-free environment. Where users can ‘try’ a service without any potential for loss they are more likely to build a degree of trust that will influence future behaviours with regard to both adoption and a sense of being ‘in control.’

The degree of control that can be exercised over personal data collected electronically is also an important factor in acceptability and adoption. We found many cases where users were deterred from using Internet sites that demanded what was perceived as excessive or inappropriate personal information for the task in hand.

“I don’t quite see why they need all this information, that puts me off.”

“Why do they need to know your correct address when you’re just registering for a news web site?”

Increased transparency and openness in data collection explaining how and why information is required and will be used is likely to enhance confidence and trust, particularly where this is combined with guarantees against misuse. In this respect legislation has an important role to play and to some extent measures are in place to protect the consumer but it is extremely difficult to exercise control across international boundaries.

“Technology is moving so fast they can’t legislate, or by the time it is legislated for it’s moved on tenfold.”

Clearly these are not simply problems that are rooted in technology; they concern the social arena in which technology use takes place and need to be addressed as such,

employing a multi-disciplinary approach that can encompass the complex and demanding issues of confident use and adoption of ICT.

Conclusion

We believe this to be one of the largest in-depth studies related to ICT engagement and the human/ICT trust relationship. The citizen-centric methodology employed in the work reported here offers an approach that provides genuine understanding of consumers' attitudes and needs that can help frame solutions to the issues we face today. We challenge the belief held by both service providers and policy makers that users need to be assured that an online service is secure before they will engage with it and we suggest that there is a far more complex trust relationship between here between user-perceived risks and user-perceived gains in ICT-mediated transactions. Being *told* that something is 'secure' is not enough to gain users trust. The findings presented here suggest that users are more likely to place their trust in something that provides safeguards and assurances for the cases when something goes wrong, rather than something that claims nothing can go wrong in the first place. Where risk can be managed, quantified or even ignored, *and* there are gains to be made in terms of convenience, time-saving, money saving, or being able to do something that they couldn't do before, the 'risk' involved is considered worthwhile *if*, and it's a very important 'if,' guarantees are in place, restitution can be made and there is minimal loss to the user.

We offer compelling evidence that challenges current thinking on how to engage citizens with ICT mediated services. 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 and uncertainty rather than building stronger security measures in isolation from the social factors that impact on technology acceptability.