2008

Security and Privacy Perceptions of E- ID: A Grounded Research

James Backhouse
London School of Economics and Political Science, james.backhouse@lse.ac.uk

Ruth Halperin
London School of Economic, R.Halperi@lse.ac.uk

SECURITY AND PRIVACY PERCEPTIONS OF E- ID: A GROUNDED RESEARCH

James Backhouse and Ruth Halperin

Information Systems and Innovation
Department of Management
London School of Economics
Houghton Street London, WC2A 2AE UK
James.Backhouse /R.Halperin @lse.ac.uk

Abstract

This paper reports on research in progress that explores the perceptions of security and privacy of UK citizens regarding electronic identity cards. In the wake of the UK National Identity Scheme proposals and with the introduction of electronic identity cards in the coming years, it is important to understand the perspectives of UK citizens. The Scheme sparked furious public debate, but as yet public opinion on the issues has not been researched systematically. Following grounded theory methods of open-coding content analysis, the findings present an empirically-grounded framework depicting the prevailing perceptions held by UK citizens. Four high-level constructs and a set of sub-categories constitute the framework that emerged: Public authorities (Competence and Integrity), Personal privacy principles (Risk/Benefit Balance, Citizen Control and A priori Anti-ID card), Legal and regulatory, and, Systems and technology. Rather than simply indicating whether citizens were 'for' or 'against' eID, the findings from the analysis uncover the reasons behind citizens' attitudes, whether positive, ambivalent or negative, and testify to the diversity of issues and concerns preoccupying them. Preliminary implications are drawn from the findings, specifically as regards the management of information and identity risk to UK citizens brought about by new identity management systems. Further directions for development of this research in progress are signposted.

Keywords: electronic identity, identity management, security, privacy, ID cards.

1 INTRODUCTION

As the move towards eGovernment gathers pace in Europe, the impact of the digitalisation of many citizen-state interactions is beginning to challenge accepted wisdom on what digital citizenship consists of, what its risks are, and how they might be managed in the new digital era. In the evolving relationship between eGovernment and the digital citizen, of growing importance is the role played by new identity management systems (IDMS) and the introduction of electronic ID cards. eGovernment projects often involve large-scale sharing of data, much of it personal data about citizens, and increasingly these projects involve the personal identification and authentication of individual citizens as they use electronic public services. (Lips, 2007, p. 38). Characterizing next generation eGovernment, Lips (2007) concludes that digitized personal identification and authentication systems, that is, IDMs, become the essential condition of successful eGovernment.

A European perspective on ID schemes shows the current diversification. In 1919, in the aftermath of World War I, Belgium became the first European country to adopt identity cards. Today, 21 out of the present 25 EU countries have some form of ID card scheme (Home Office 2006), which are paper-based systems. The four countries currently with no ID cards are the UK, Ireland, Denmark and Latvia. Of the 21 countries with ID cards, 10 ostensibly have voluntary schemes; however, the degree to which they are actually voluntary varies. For example, although people residing in France are not technically required to hold an ID card, it is virtually impossible to get by without one as they are connected to important administrative systems, such as state benefits (Beck and Broadhurst 1995). ID card schemes in the EU vary along other dimensions, such as powers given to authorities demanding to see them and in their functionality. For example, most ID cards only hold basic information such as name, address and a numerical identifier and are not linked to a central database. The UK Home Office in 2004 caused uproar by proposing an "entitlement card" holding highly personal information such as biometric data and health care records, with the possibility of adding other items, such as bank details. The UK plans for the entitlement card have now been scaled back to include only basic personal and biometric data, and the government is moving away from hosting the only ID card scheme that includes a central database[1].

In the midst of much discourse about the functionality of such systems, often ignored is the necessity for considering the perceptions and concerns of the citizen about new technology that deploys identity management in the context of eGovernment. The term "citizen-centric" has been developed[2] to refer to this aspect of the emerging systems, an aspect that may vitally affect whether or not such systems win public acceptance. The eventual institutionalisation of eGovernment systems will almost certainly require that they prove to be amenable and acceptable – i.e. citizen-centric. Time and again large-scale systems prove to be eventual failures as a result of resistance from end-users during the phase of implementation (Bauer, 1997). A major research programme in the UK entitled 'ensuring privacy and consent in identity management infrastructure'[3] could epitomize a recent change of heart on the part of

[1] http://www.silicon.com/research/specialreports/idcards/0,3800010140,39164756,00.htm

[2] http://www.digitalchallenge.gov.uk/links-and-resources/research/study-on-organisational-change-for-citizen-centric-egovernment

[3] http://www.kablenet.com/KE.nsf/EventsSummaryView/0CFE397AFD0FF888802572E50050D62B?OpenDocument

the UK government in implicitly recognising that without consent acceptance will be difficult to win.

Indeed, research into citizen security and privacy perceptions in the UK is of paramount importance in the wake of the National Identity Scheme (NIS) and, in the coming years, the introduction of eID cards. The NIS gave rise to a fierce public debate in the UK with privacy concerns being aired by civil rights movements (Crossman, 2007) and with serious doubts arising on the costing, legality and security of the scheme[4]. Yet little attention has been paid to the perspective of the UK citizens.

The research reported in this paper examines the security and privacy perceptions of UK citizens with regard to eID. The study seeks to understand citizens' attitudes towards the introduction of new technology for identity management and more specifically to reveal the reasons behind those attitudes, whether positive, ambivalent or negative.

In this introduction we have presented the rationale underlying this research, highlighting the pertinent need for studying security and privacy issues as perceived by citizens. This is contextualised within the UK NIS, which spurred public debate, but as yet public opinion has not been examined systematically. The risks and concerns as perceived by citizens deserve attention and consideration: citizens are the ultimate sponsors and ought to be the beneficiaries of any government identity scheme. Furthermore, citizen perceptions hold important implications for any future attempts at implementing eID cards, as these perceptions may well be translated into subsequent behaviours, namely, resistance to use misuse, or non-use.

The remainder of this paper is structured as follows. The next section introduces the methodology used in the study. We explain why we have chosen a qualitative interpretivist approach to guide this study, describe how we collected the data and used a grounded research method for analysis. Then follows the main part of this paper, introducing and illustrating the findings of this research in progress. The empirically-grounded framework that emerged from the analysis uncovers the diverse set of security and privacy perceptions held by UK citizens as regards eID. This is followed by a preliminary discussion of the implications arising from the analysis. We propose that the management of risk attached to identity management systems (IdMS) in eGovernment warrants a thorough examination. More specifically, the key issue of redress or restitution must be addressed and resolved in order for risks to be managed, as current practices and divisions of responsibilities and accountability fall short of adequately securing the citizen. A reappraisal of responsibilities between eGovernment and digital citizens is called for. We conclude the paper by summarising the key findings arising from the study and by indicating directions for continuation and expansion of this research in progress.

2 METHODOLOGY

The methodology adopted in this study drew from Grounded Theory (Glaser and Strauss, 1967; Martin and Turner, 1986) as it offers a research method that seeks to develop accounts that are grounded in data. This generative approach seemed particularly useful here given that no systematic research on this topic has been published to date. In particular, we adopted the analytical technique of open coding (Strauss and Corbin, 1990) as explained further in section 2.2 below. This method provides for an exploratory and context-based research into the phenomenon at hand.

[4] http://identityproject.lse.ac.uk/identityreport.pdf

The inductive and contextual characteristics of the methodology suggested by Grounded Theory fit with the interpretive, rather than positivist, orientation of this research. The focus here is on developing a context-based description, with an aim of generating an account of UK citizen security and privacy perception as regards eID.

2.1 Data collection

This study as research in progress is carried out as part of a 5-year collaborative research project entitled FIDIS[5] (the Future of Identity in the Information Society) funded by the European Union. While a wide range of topics and themes are being studied within this framework, the study reported in this paper was designed specifically to address attitudes and perceptions of citizens towards eID. In this context a survey was launched entitled "A survey on citizens trust in ID authority and systems"[6]. This web-based closed questionnaire produced a significant response for the quantitative analysis contained in the research deliverable cited. The overall number of valid responses from UK and Ireland citizens was N=379.

The data set that forms the basis for the empirical study in this paper derives from an open-ended question at the end of the survey questionnaire which invited respondents to comment freely on the issues forming the subject of the survey. This generated a wealth of quantitative data - statements made by respondents in the form of free text, for example:

> *I am less concerned about ID card per se, as about a centralized database…*
>
> *Security will only be as strong as the weakest link, and there will be a vast amount of links in this chain, I have very little faith that the weakest one will be up to the task.*
>
> *ID cards and the NIR in the UK are an infringement of our civil liberty and lessen our freedom*

Apart from three respondents who responded to the survey but did not provide any further comments, all other respondents from the UK had replied to the open-ended question by freely commenting on the survey and the issues surrounding its topic. Statements varied in terms of length and their level of elaboration, for example, one respondent stated: *'1984'* whereas another explained in more details:

> '*It's an absolute necessity to pare the amount of centrally stored electronic data to the absolute minimum. Especially cross-comparison of different data bases must be permitted by law, just as access to this data by companies/business. Additionally, it must not be possible to read out electronic data stored on regular ID cards by radio frequency or any other contactless method, because every encoding, encryption or access protection will be cracked, which is just a question of time. Business/companies, banks and insurances have economical interests to get access to this data, so that access must be permitted by law. With these constraints I would agree to electronic ID cards'.*

[5] www.fidis.net

[6] Report available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.4.survey.pdf

2.2 Data analysis

Making sense of this large body of unstructured text required the creation of a grounded analysis framework. Content analysis of the text slowly led to the creation of a framework of underlying reasonings or beliefs that characterised the range of responses and attitudes. This technique uses a form of content analysis where the data are read and categorized into concepts that are suggested by the data rather than imposed from outside (Agar, 1980). This method of open coding (Strauss and Corbin, 1990) relies on an analytic technique of identifying possible categories and their properties and dimensions. As the data are examined, concepts are organized by recurring themes. These themes became prime candidates for a set of stable and common categories, which link a number of associated concepts. This is known as axial coding (Strauss and Corbin, 1990) and it relies on a synthetic technique of making connections between sub-categories to construct a more comprehensive scheme. The goal is to determine a set of categories and concepts that covered as much of the data as possible (Orlikowski, 1993). This iterative examination yielded a set of broad categories and associated concepts that described the range of responses and perceptions held by UK citizens. Using this emergent framework each response could be assessed in terms of positive, ambivalent or negative towards the common set of elements. In effect the research produced a data-driven, rather than a normative, framework of reasoning for attitudes on electronic ID, interoperability and trust. At the highest level the perceptions of citizens revolved around four broad concerns: public authorities, personal privacy principles, legal and regulatory issues and systems and technology. In the next section we provide a high level presentation of the framework. We then introduce the refined categories by turn, illustrating each one with the data from which it emerged.

3 FINDINGS

The grounded analysis of the data set gradually gave expression to a number of high-level constructs that were slowly narrowed down into a manageable handful of framework elements. As the analysis proceeded, the categories were refined into an ever-smaller number of these elements. We felt that the framework needed to be simple but high-level in order to capture as wide range as possible of citizens' perception within that smaller set of constructs. Furthermore, we wanted the elements to lend themselves to the evaluation of respondents' attitudes along a continuum from positive to ambivalent to negative. We now present a high-level introduction to the framework that was refined in this manner.

Public authorities were seen as a key actor in the perceptions of citizens regarding eIDs. Citizens held well-defined views on the *competence* of the state and government departments in securing and managing personal data. The state's institutional ability to provide high standards of professionalism in respect of the management and use of IT systems was seen as necessary for fostering a sense of trust regarding the security of personal data in safeguarding against fraud, abuse and human error. Alongside competence, the *integrity* of public authorities ranked high with citizens, concerned about questions of truthfulness and fairness from the institutions of the state in respect of their handling of personal data.

As well as the issues concerning public authorities, there emerged clear notions of deeply felt *personal privacy principles* such as the balance of risks and benefit to the citizen, the ability to control personal data and, in the UK at least, a-priori positions against an ID card. In the case of the risk and benefit balance, the issue was a pragmatic question of whether the perceived benefits outweighed the perceived risks. This was an issue in the area of interoperability, or the sharing of data, between departments or across states of the European Union in regard to mobility within Europe, especially when benefits were weighed against the risks to privacy. The control principle indeed intersects with the balance principle for the informed choice of adequate balance rests on consensual agreement, the cost to the

individual, and the level of interoperability or sharing of data. Greater clarification was sought on the type and amount of data gathered and why, on the system to be used, on the security surrounding the data, on the citizen's ability to correct misinformation, on business and government interests, and overall cost. Conspiracy theories ranged from state control of dissenters and immigration to super-intrusion into people's lives, with high likelihood of breaches of privacy.

Many respondents recorded their a-priori beliefs about the value of an ID card, regardless of the scheme or the arrangements for its implementation. It allowed proof of identity, although one view saw it predominantly as emblematic of a modern form of dictatorship, or authoritarian police state, an undemocratic instrument for population control, micro-management and surveillance and as such, as constituting a fundamental infringement of civil liberties and abuse of personal information, heralding a shifting balance of power away from the citizen towards the state.

As might be expected, legal and regulatory matters were given some importance. There was a feeling that the necessary laws and regulation should be in place, with occasional requests for more powers for commissioners to intervene in the case of abuses. In particular there was a need felt for legal protection against the incursions of commercial interests into publicly-held personal information.

Another dimension that emerged was the issue of systems and technology. Although technology was seen to be more dependable than in the past there were fears about the robustness of identity management systems in particular. Centralised databases, biometrics and wireless technology, vulnerable open standards that interoperability often requires together with the lack of platform independence – all were mentioned as examples of reasons why citizens should fear the large-scale deployment of interoperable electronic IDs. The visibly low success rate for large public-sector IT projects in the UK was cited as further proof of this reason to be afraid.

As outlined above, four high level categories constitute the grounded framework depicting security and privacy perceptions of UK citizens towards eID. These consisted of: Public authorities, Personal privacy principles, Legal and regulatory, and, Systems and technology. In the sections that follow we present each category in turn, providing illustrations from the data analysed.

3.1 Public Authorities

As far as public authorities were concerned, attitudes in the data set divided into two broad areas of interest: competence and integrity. Attitudes in the United Kingdom regarding the competence of public authorities in respect of IT systems have been strongly coloured by some startlingly poor performances in recent years. There have been a number of high-profile technology projects in the public sector that have failed miserably, such as the 2 CDs with 25m records lost by Her Majesty's Revenue and Customs office[7], the Child Benefit Agency database or the present difficulties being experienced by the world's largest IT project, NHS Connect (Brennan, 2007). A further worry in the NHS case is the perceived inability to assure information security in a context where perhaps 300,000 NHS employees will have access to a central database of some 60 million records:

> *I believe the authorities will attempt to be honest and secure but ultimately will be unsuccessful in maintaining the confidentiality of my data*

[7] http://news.bbc.co.uk/1/hi/uk_politics/7104945.stm

Here there is an unrelenting pessimism about the state's ability to maintain confidentiality, notwithstanding some belief in its good intentions. Examples of security failures are legion, such as NHS staff, despairing of the lengthy authentication procedures, routinely breaching security policy by sharing smart cards when accessing patient records[8]. Security failures such as the breach at the UK tax credit web site of summer with losses of £30m, or the recent HMRC data breach debacle mentioned above, undermine belief in competence of public authorities to deal with information risks and implement appropriate security. Indeed the worrying issue in the former case was that criminals used identity information stolen from 1500 Department of Work and Pensions staff, and this does not bode well for citizens if the very staff themselves have their personal information stolen.

> *I feel the authorities will fail to deliver a secure, working system. It will be a monumental waste*

> *I am not against ID cards in principle, but have grave doubts about the competence of those running the system. Human error is probably a bigger risk then IT*

This response does not oppose the ID card in principle, but shows no faith in the management abilities of public authorities to secure against information risk. Neither does it locate the problem with technologies but rather with the failures of the social and organisation aspects of managing information risk and security.

Alongside concerns about the competence of public authorities in managing information risks in public information systems lies a further concern for their integrity, or lack of it. One view that emerged was of a government, notice not the state, hell-bent on giving UK personal citizen information to third parties without any notice.

> *…our Government will hand over our data to the CIA or any other organisation they care to without telling us*

Here the background is that there are cases of where personal information has been made available to third parties without the citizen necessarily being aware. Examples might include information on the Electoral Register that is sold commercially. There are cases of information held by the UK Driver Vehicle Licensing Authority (DVLA) also being marketed, and of course, the best example is found in the United States where medical data, albeit anonymised, is routinely sold to insurance companies. Such concerns are evidenced in the following statement from one respondent:

> *I am very concerned about the misuse of ID information especially considering links between government and industry*

Here again we find that it is the perception itself that is damaging, even though the reality may or may not support that perception. Once there is a belief abroad that the state cannot be trusted to safeguard personal information, it becomes very difficult to shift it.

3.2 Personal Privacy Principles

The second element in the framework developed is that concerning the principles held by citizens in respect of privacy. Although our data set numbered some very strongly held positions on aspects of personal privacy, the aim of developing the framework was to identify the dimension on which that strongly held belief could be located as positive, negative or ambivalent. In this way each response could be interpreted in a similar vein by adopting the

[8] http://www.pulsetoday.co.uk/story.asp?sectioncode=23&storycode=4115280&c=2

frame. One area that cropped up time and again was the issue of citizen control of personal information held by the public authorities, and others. This is a feature of many identity management systems in which the data subject has the power to, and in some cases is responsible for, keeping her personal information up-to-date and correct. For example, the online UK self-assessed tax declaration system hosted by HMRC asks the user to enter relevant changes to her profile as soon as authentication is completed. What some citizens fear is not knowing what data is being held, whether it is accurate, honest and appropriate for the purpose. As society becomes ever more information-intensive, a mistake in a personal record might have dire consequences – as we find in credit reference cases where the subject has been blacklisted for mortgages and loans but has no idea why. From some respondents came a clear pragmatism that eschewed an entrenched contrary position, but rather looked for the justification regarding the case itself.

> *No objection in principle but depends quite a lot on the type of data held…*

But there were those who rejected wholesale the idea of the government managing their data. Here there may be some confusion between government and state, as these terms tended to be used interchangeably. Of course particular governments change regularly but the state tends to be a much longer-lasting entity.

> *As a citizen I have virtually no say in what the government does: or a quick and easy way to control it…I don't want them managing my own data*

This last quote mentions the idea of ease of control that broaches onto the subject of the kind of interface to any citizen control systems that might exist. For the average citizen who has no expertise in using secure information systems, the difficulty of access could be a critical matter and hence the ease of use issue is an important one.

Another factor in the personal privacy principles element is that of the risk/benefit balance. Many citizens appreciate the potential benefits of a more joined-up government with better access to personal information thorough ID cards which,

> *if implemented correctly could make general travel and access to public services more convenient*

and also, for example, might reduce the number of times they are asked to fill out forms requesting the same data. If, say, the accurate data on the tax system could be available to other branches of government perhaps this would speed up the machinery of state - goes the logic. Unfortunately citizens also perceive a downside in which the information risks are heightened once the value and usefulness of that information are enhanced. Many risks to confidentiality, availability and the integrity of personal information on public authority databases have been confirmed. If key medical data were to be leaked, this might result in the inability to obtain insurance, or again if identity information were to be stolen, it might be extremely difficult to retrieve the situation in the short term, leaving the victim without the ability to authenticate herself in important situations. Much of the risk to citizen's personal data will be beyond the ability of the individual to manage. The risk will be to data held in government department databases and under the control of public systems security managers. Looking at balance between benefits and risks implicit in the large-scale deployment of interoperable electronic IDs, different citizens find different trade-offs, but for many the calculation is a constant consideration.

It may have been the timing of the survey, mid 2006, during the lively UK National ID cards Bill public debate, but there were strong feelings that emerged regarding the very existence of IDs in the United Kingdom. Typical of this genre was the following quotation that conflates the very notion of an ID card with oppressive government:

The idea of a general ID card for all citizens is very wrong…it is a modern form of dictatorship and basically not a fair system..

This was an example of a deeply held a-priori belief that saw ID cards as anathema to democratic society. Although a view that would be impossible in many countries throughout Europe, it is still found alive and well inside the UK, despite the UK's now notorious affinity for CCTV and similar surveillance practices (Wood, 2006).

3.3 Legal and Regulatory

The feedback on the legal and regulatory question highlighted the uncertainty about whether the appropriate framework was in place. There were statements that asserted positively, negatively and ambivalently on this question. One view came down to the idea that the main issue was about learning to get along with the legal framework and not about whether it existed or not:

…the legal structures are in place…people just need to get on with understanding and adhering to them…

While at the same time an ambivalent view held that more legal and regulatory buttresses need to be put into place to address the economic arguments for wider access to personal information:

Legal structures and regulation are in place but legal protection against economic access must be guaranteed

Yet again, an entirely negative view intimates that the necessary legal framework needs yet to be introduced, asking the question of whether appropriate protection would be introduced by legislators:

Would laws be made out of it, which prevent the state and all others from collecting personal data and use them against the affected persons?

3.4 Systems and Technology

On the question of systems and technology, mainly concerning dependability of the technology, there were diametrically opposed views to be found. Some were adamant that biometric based ID cards offered unbreachable security,

Biometric based ID cards are secure as only you can provide the live match with biometric stored on the card, therefore the information help is useless without the individual present…

whereas others had a very poor estimation of the possibilities for reliable technology in the identity management systems area. The feeling persisted that the claims being made for the effectiveness of biometric based ID technology would have to be confirmed by lengthy testing in live contexts that were less critical.

I do not believe such a (safe) technology exists, nor that it can be proven to exist without many years of use in a less critical mission application

Others decided to sit on the fence and to side neither with the former nor the latter, instead remaining ambivalent about the dependability of the systems and technology in this specialized domain.

Electronic ID provides many benefits and are (probably) technically realizable but doubts remain about the integrity of the IT system…

Although many had remarks to make about the technology, few held the view that it was a deciding, or even the most important factor.

4 PRELIMINARY DISCUSSION AND IMPLICATIONS

The information-intensive society that is emerging in modern times seems now to be converging with a 'personal information economy' (Lace, 2005). Not only does information drive how products and services are produced and distributed, but increasingly it is *personal* information that is the motive force. Governments are learning fast from the techniques being adopted in commercial businesses and are using similar models, systems and technology to deliver government services. The problem, in the UK at least, seems with the policy and architectures chosen for eHealth and for eGovernment that gather vast amounts of personal information but need to provide operational access to, in the case of the NHS, hundreds of thousands of employees. Neither security technology nor security management can satisfactorily address the information risks implicit in these architectures. The more that services, and in particular benefits, are accessed through IDs and identity-based information used in passwords, the more valuable does the possession of IDs and such information become. Higher value IDs mean greater risks to their security. A poorly paid public servant can easily be attracted by the sale value of such information or by the rewards from organised crime for turning a blind eye where necessary. Hackers are especially motivated by the rich rewards for cracking network protection.

But where does this leave the ordinary citizen? The citizen is being told that electronic IDs are essential to efficient modern governmental systems and is being encouraged to interact with the government through electronic means, and in particular through the internet. Moving to this model of government-citizen interaction however enormously raises the risks for the citizen, especially risks related to identity fraud. Such risks include financial loss from bank accounts and state benefits wrongly claimed by another, and also considerable personal distress associated with the difficulty of establishing unequivocally one's identity if security is compromised. Although raising the risks to the individual, the state has not proposed any solutions for this higher risk profile. A report from the UK Treasury by Sir David Varney[9] argued that how the state manages identity must address the needs and concerns of the person who owns that identity. It articulated an "Identity Management Vision": that identity must be secure and trusted. It called for a clear governance framework for identity including mechanisms for dealing with updates, errors, record repair after fraud, for liability and remedy when things go wrong. The difficulty arises with the consistently poor performance of the state in this area. All the good intentions – rules, procedures, processes, standards – in the world mean nothing if the actual behaviour and performance does not match them. There is a crisis of credibility. Citizens in the UK find great difficulty in trusting a state that continually lets them down.

There is another important element in this convoluted context. The ID issue was always interpreted solely in terms of the technology that government departments deploy, and never involved a reflection on the responsibilities of citizens who interact with the public databases. In the rush towards electronic access with cheap broadband channels, the issue of the security of the individual citizen's domestic information systems has been somewhat overlooked.

[9] http://www.hm-treasury.gov.uk/media/4/F/pbr06_varney_review.pdf

What responsibility, indeed liability, should citizens have in ensuring that their home computers do not form part of a "botnet" that is being used by organised criminals to attack commercial web-sites with denial of service attacks, to disseminate spam designed to place keystroke sniffers on the hard disks of unsuspecting citizens, or indeed to support ramping and other market malefaction? An unsuccessful attempt in 2002 in the UK tried to introduce a private member's bill that placed legal liability on the citizen to maintain antivirus and other security on their systems. This might be something worth considering afresh.

5 CONCLUSION AND CONTINUATION OF STUDY

This paper reported on a research in progress exploring security and privacy perception of UK citizens regarding electronic identity cards (eID). Drawing on Grounded theory methodology, the qualitative data collected was examined using open coding content analysis. This analytical process developed a grounded framework depicting prevailing perceptions held by the citizens. Four high-level constructs and a set of sub-categories constitute the emerging framework: Public authorities (Competence and Integrity), Personal privacy principles (Risk/Benefit Balance, Citizen Control and A priori Anti-ID card), Legal and regulatory, and, Systems and technology. Rather than simply indicating 'for' or 'against' eID, findings emerging from the analysis uncover the reasons behind citizens' attitudes, whether positive, ambivalent or negative and testify to the diversity of issues and concerns preoccupying UK citizens in the e-ID context.

In the wake of the NIS and with the introduction of eID cards in the coming years, it is pertinent to understand the perspectives of the UK citizens. Knowledge of the concerns and expectations of citizens can and should be used to inform the design of future IdMS and related e-government services. Furthermore, underlining citizens' reasoning and beliefs should shape and improve the much-needed dialogue between policy makers and citizens around a topic which raises controversy and strong emotions.

One important issue highlighted by this research in progress concerns the ever-increasing risk to the citizen brought about by new Identity Management Systems (IdMS), while the current practices and divisions of responsibilities and accountability fall short of adequately securing the citizen. Redress for victims of IdMS must be addressed and resolved for risks to be managed and this suggests reappraisal of responsibilities between eGovernment and digital citizens – perhaps towards a social digital contract in the UK, setting out rights and responsibilities, duties and liabilities? This is one avenue we propose in further developing and expanding this research in progress.

Additional developments of this research also include refinements to the analytical framework as well as theoretical development, specifically by proposing and employing a theory of interpretation and in so doing shifting the focus of the analysis from grounded theory to theory driven. This, we propose, should provide further insight into the pressing contemporary issues associated with eID and increase understanding of citizens' perceptions of it – both their concerns and expectations.

6 REFERENCES

Agar, M.H. (1980) The Professional Stranger: An Informal Introduction to Ethnography. New York, NY: Academic Press.

Bauer , M. (Ed.). (1997). Resistance to new technology: nuclear power, information technology and biotechnology. Cambridge: Cambridge University Press.

Beck, A. and K. Broadhurst (1995) *National Identity Cards in the European Union: The British Debate,* Centre for the Study of Public Order, Leicester.

Brennan, S. (2007). The biggest computer programme in the world ever! How's it going? Journal of Information Technology, 22, 202-211.

Crossman, G. (2007). The ID Problem. In D. Birch (Ed.), Digital Identity Management (pp. 175 - 183). Hampshire: Gower.

Glaser, B.G. & Strauss, A.L. (1967) The Discovery of Grounded Theory: Strategies for Qualitative Research. New York, NY: Aldine.

Great Britain Home Office (2006) *Why We Need Id Cards* Great Britain Home Office http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/why-we-need-id-cards/.

Lace , S. (Ed.). (2005). The Glass Consumer: Life in a Surveillance Society, Policy Press.

Lips, A.M.B., (2007) 'E-Government Under Construction: Challenging Traditional Conceptions of Citizenship', in P. Nixon & V. Koutrakou (eds.), *E-Government in Europe. Rebooting the State*, Routledge, London, pp.33-47.

Martin, P.Y. & Turner, B.A. (1986) Grounded Theory and Organizational Research, The Journal of Applied Behavioral Science, 22:2, 141-157.

Orlikowski, W. (1990) CASE tools are organizational change: Investigating Incremental and Radical Changes in Systems Development, MIS Quarterly, 17:3, 309-340.

Strauss, A. & Corbin, J. (1990) Basics of Qualitative Research: Grounded Theory, Procedures, and Techniques. Newbury Park, CA : Sage.

Wood, D. M. (Ed.). (2006). A Report on the Surveillance Society, Information Commissioner office, UK.