2009

Exploring the Issues of Security, Privacy and Trust in eGovernment: UK Citizens' Perspective

J. Choudrie
University of Hertfordshire, j.choudrie@herts.ac.uk

S. Raza
University of Hertfordshire

P. Olla
Madonna University

Exploring the Issues of Security, Privacy and Trust in E-Government: Uk Citizens' Perspective

Choudrie, J.[1], Raza, S. University of Hertfordshire, Business School, DeHavilland Campus, Hatfield, Herts. AL 10 9AB.

Olla, P., Madonna University, 36600 Schoolcraft Rd. Livonia . Michigan, 48150.

INTRODUCTION

Recognising the potential that Information and Communications Technologies (ICTs)[2] offer for competitiveness and the effectiveness of communities, Governments across the globe are striving to provide online products and services[3] to all user groups. There are various definitions of e-government within the literature, and the one being applied in this research is: E-government is the application of technology to enable, enhance and improve access to the delivery of government services for the benefit of citizens, employees and enterprise (Silcock, 2001)

Whilst there are diverse definitions of e-government, there are also variations in the classification of e-government, each dependent upon the relation between the various stakeholders. Bélanger and Hiller (2005) classified e-government into six categories: Government Delivering Services to Individuals (G2IS), Government to Individuals as a Part of the Political Process (G2IP), Government to Business as a Citizen (G2BC), Government to Business in the Marketplace (G2BMKT), Government to Employees (G2E) and Government to Government (G2G). G2IS involves communication and services between government and citizens (G2C); G2IP involves the relationship that the government has with citizens as a part of the democratic process, such as e-voting. G2BC involves organizations paying taxes or filing reports, and G2BMKT focuses on business transactions between government and businesses, such as e-procurement.

Electronic interactions between Government and Citizen can also be classified as a 'Government to Citizen' (G2C) model of eGovernment (Beynon-Davies: 2007). This is also referred to as the 'Transactional' stage of eGovernment, where the interaction can occur with an agency (NAO, 2007). This interaction involves the receipt or dissemination of information, the completion or submission of a form, the sending of payments, the inspection of an account, or more complicated sets of dealings. It is such transactions that can be perceived to be of sensitive nature for citizens and users are reluctant to conduct transactions, with concerns ranging from: payment security, not understanding how to integrate information and customization impacting their privacy (Belanger & Hiller; 2005). This leads onto security and privacy and their possible effects on transactional stage adoption.

In this research paper *the aim is to explore how UK is dealing with the issues of security, privacy and trust when adopting and using online government products or services*. This is pertinent at this time as the government is taking large steps to increase adoption and usage amongst citizens. By undertaking this research, several contributions are made: Governments around the globe, including, UK are increasingly seeking success at e-Government adoption and usage and such research assists policymakers in obtaining a better understanding. For industry, private sector organizations are partners in the provision of the infrastructure and involved in many other implementation and adoption e-Government projects and research such as this allows them to consider these factors in more depth. For academics, security, privacy and trust are issues of immense importance and research such as this allows academics to become more aware of these topics.

---

[1] Contact Author:j.choudrie@herts.ac.uk

[2] Examples of ICTs include Broadband (the offering of a faster internet service), internet, personal digital assistants, such as, blackberries and mobile telephones

[3] There are various definitions of e-government, but for the purposes of this research, the definition used is: E-government is more commonly known as the the provision of online products and services

This research paper is structured as follows: A theoretical foundation of this research is offered in section two. Section three then details the research approach. Section four offers the findings of this research and section five, the analysis and discussion to this research. Section six concludes this paper and also offers some future directions and limitations' of this research.

BACKGROUND

Previous experience of eGovernment systems in the UK

The Cabinet Office (2008) defines eGovernment delivery as an ongoing endeavour and as such the eGovernment initiative is being delivered through programme management practices as developed and subsequently refined by the Office of Government and Commerce (OGC). Strategic objectives are being initiated, planned, integrated and resourced through programme management; for which the OGC's (2008) Managing Successful Programmes (MSP) framework is being utilised. The principal vehicle for delivering these goals is the Projects in Controlled Environments (PRINCE2) methodology, which is also owned by the OGC, as is the procurement capability of the Government. The widespread use of project management as the vehicle of change is part of the Government's wider campaign to pursue a more commercial image with the citizen being considered as a customer (Cabinet Office: 2007).

When considering e-government delivery lack of trust was seen to be a major barrier, citing fears about security and privacy are inhibiting eGovernment adoption across the European Union (The Barriers to adoption report, 2007). The report also proposed an action plan to manage the trust tension through technical solutions including the improved authentication and identification of users while online (ibid). It is not clear whether the Government has the technical expertise or capability to fully pursue these resolutions given the report also signposted the holistic nature of the barriers.

Security, Privacy and Trust Perspectives in e-Government

Security and trust have been examined in previous e-government research where the foundations were laid by comparing e-government and e-commerce[4] (Carter and Belanger, 2005). It has also been noted that there are 3 distinct differences; access, accountability and structure (Jorgenson and Cable, 2002). For instance, the service delivery strategy of www.amazon.com cannot fully be applied to transactions on www.direct.gov as users may not be willing to divulge information on a government site due to a lack of trust on the citizen's part (Beynon-Davies: 2007). The complexity of service delivery in the public sector (breadth of stakeholders) means the provisioning of e-commerce and e-government services require different planning approaches (Jorgenson and Cable, 2002). The delivery of citizen centric services is enabled through, what are classified in the UK as transactions (or transactional services) that exist between the government and UK citizens (NAO, 2007). Transactions or transactional services are defined as an interaction with an agency; this interaction could be the receipt or dissemination of information, the completion or submission of a form, the sending of a payment, the inspection of an account, or more complicated sets of dealings (NAO, 2007).

Security, in the Information Systems (IS) context describes the processes that define who may interrogate or modify a computer system or the information contained within (Saltzer & Schroeder, 1975). It also describes the ways IS may be vulnerable to a range of conscious attacks in which the effectiveness and/ or integrity could be compromised and in response to such attacks, the use of a policy and processes employed to detect, respond and protect a system with a focus on confidentiality, integrity and availability (CIA) (Dourish & Anderson: 2006).

Westin (1967) defined privacy as the desire of people to have the freedom of choice under whatever circumstances and to whatever extent they exposed their attitude and behaviour to others. It denotes a socially defined ability to determine whether, when and to whom information may be revealed (Saltzer & Schroeder, 1975). Additionally, it can be interpreted as the way by which individuals or organisations might lose control of access to information (Dourish & Anderson, 2006). Privacy then, is a social consideration; whereas, security is the technical consideration (Dourish & Anderson: 2006). This association requires the balancing of risk against cost (Egan and Mathen, 2005).

Trust is a broad based concept for which there are many interpretations. For the purpose of this study, the term 'cybertrust' as defined by Dutton and Shephard (2006) will be used. Cybertrust is defined as trust in the Internet and related information and communication technologies (Dutton & Shephard, 2006), which could be critical to the successful delivery of eGovernment initiatives (Beynon-Davies: 2007). Belanger et al (2002) viewed trust as 'the perception of confidence in the electronic marketer's reliability and integrity' and is not too dissimilar to Dutton & Shephard's (2006) interpretation. Park's (2008) work on the values and decision making that lead citizens to use e-government services instead of traditional

[4] E-commerce is identified as the selling of products or services to customers using the internet as the main means for communication and accomplishing transactions

government delivery channels reveals that public trust in eGovernment is a primary input of transactional usage. Dutton and Shephard (2006) concur that the internet is an experience technology, suggesting that trust and experience affect each other. This is significant because it suggests that there must be a degree of cybertrust present in a citizen before developing cybertrust amongst eGovernment services. A study of eGovernment accountability in UK found that one of the principal stakeholders identified by respondents was citizens. In turn, they felt they should be involved in scrutinising services (Griffin & Halpin, 2005), however it was also understood that citizens were never represented at eGovernment project meetings. This trust tension needs to be balanced and can be viewed as the tension between the need to collect the data of citizens to provide and improve eGovernment services and the fear of citizens in the Government using data for surveillance and other inappropriate purposes (Barriers to Adoption Report: 2007). Measures for building trust for eGovernment can further be interpreted as the risk management of: identity theft, safeguarding personal information, privacy risks, transaction security and the sharing of personal information (Park, 2008). For a citizen to use eGovernment services in a transactional state, access through the internet is a fundamental requirement. Therefore, a degree of cybertrust in the internet would be required before any transaction can occur and the success or failure of risk management on the Governments part could influence this.

Evidence from archival sources suggests that Government is just beginning to realise the challenges and complexities of the eGovernment programme. These concerns emphasised citizens being sceptical and mistrusting eGovernment initiatives. (James, 2000; Thibodeau: 2000). Research conducted by Norris and Moon (2005) found a major barrier to eGovernment adoption as being issues related to security, lack of technology or web experience and issues regarding privacy.

Diffusion of Innovations Theory

To examine e-government related issues, a favoured theoretical model is the Diffusion of Innovations (DOI) model developed by Rogers (1995). Mason and Hacker (2003) concur that DOI is a most appropriate theory for analysing the adoption of new innovations. DOI is a model that makes the proposition that an individual's decision to use a new concept or technology is based on the perception of the new concept or technologies characteristics. Diffusion refers to the dissemination of an innovation into society and an innovation is considered to be new concept or technology (Rogers, 1995; Carter and Weerakkody, 2008). In this case the innovation being modeled for diffusion (by citizens) is the eGovernment G2C transactional stage.

According to DOI theory the characteristics of an innovation can help understand the rate of its adoption. There are five characteristics that influence a potential citizens adoption of G2C; relative advantage, complexity, compatibility, trialability and observability. Relative advantage is one of the principal characteristics of DOI theory and is defined by Rogers (1995) as the degree to which an innovation is better than that which it supersedes. It is the belief that an innovation is more useful than its predecessor, it is the perceived improvement over the previous innovation and the greater the perceived advantage, the faster the adoption. Complexity is the ease by which a potential adopter can understand and use an innovation. It is the perception of difficulty associated with the innovation and Roger's suggests that more complex innovations take longer to be accepted and used. Compatibility is the characteristic that interprets the performance of an innovation in the context of an adopters experience, value system, customs and needs; Trialability is the measure of how an innovation can be assessed and tested by a potential adopter prior to fully adopting that innovation. It is posited that the greater the level of trialability, the faster the rate of adoption. Finally, observability measures the level of tangible benefits of an innovation, with the view that readily observable innovations are adopted at faster rates.

The DOI theory hypothesizes that as the measure of each of these characteristics increases, there will be an increase in the adoption of an innovation with the exception being complexity. Rogers (1995) states an increase in complexity results in a decrease in adoption. Agarwal and Prasad (1998) cite that of the five DOI characteristics, three are most supported by empirical studies-relative advantage, compatibility and complexity. Carter and Weerakkody (2008) suggest that it is relative advantage that stands out as consistently being a principal factor of technology adoption. Relative advantage is also a principal theoretical construct of another widely used model; the Technology Acceptance Model (TAM) (Davies, 1989). TAM theory constructs are included in the DOI model (Venkatesh et al, 2003). However, Tornatzky and Klein (1982) conducted a robust meta-analysis of adoption paradigms and found that relative advantage was in fact a weak and non-specific variable that has too broad a connotation to be a respectable marker for adoption. However, this is contrary to when it is used as a specific measure such as potential cost benefit to adoption (Tornatzky and Klein, 1982). Consequently, it will still be applied due to its wide use as a marker for eGovernment adoption. In the case of this research, the construct of relative advantage will be illustrated as a more directional marker as recommended by Tornatzky and Klein (1982). The authors also recommended the need to study additional variables to synthesise findings from the constructs. DOI constructs have been used in many studies to as a paradigm to measure the status of eGovernment adoption (Carter & Belanger, 2004; Gilbert et al, 2004; Norris & Moon: 2005; Choudrie et al, 2007; Mirchandani et al, 2008). The adoption models used in these studies have

all implemented some or all of the following constructs in their respective adoption models/ studies; perceived usefulness (relative advantage), trustworthiness, internet skill, privacy, involvement and the intention to use (as the dependent variable).

RESEARCH DESIGN

Carter and Belanger (2005) also examined trust and security in e-government but in the USA and at a time when security and trust were becoming issues of concern. This research is different in that it examines security and trust in the UK, mainly in light of several government efforts that have been undertaken to address these issues. As an example, previous years have seen UK citizens use the internet for the completion of their tax returns, with large numbers of citizens using the traditional mode-postal service. However, this year, 2009, the government ensured that there would be improvements to its IS, an increase in the awareness of using online tax forms with further incentives for citizens in using the online tax system, including, reductions in payments if online tax forms were employed. This has resulted in increases in the numbers of online completed forms to 40% this year. Between April and December 2008, nearly 2.8million forms were received online, compared to 1.9 million in the same period last year. Just over 2.6 million returns were received by post. HMRC expects 58% of customers to use the online service this year (Thomson, 2009).

To form a foundation for the research direction, a literature review was conducted. Then a survey was conducted. Prior to undertaking the survey, a pilot study was undertaken by distributing the questionnaire amongst ten carefully selected individuals. Five from academia and five professional services' practitioners (comprising of management consultants and information security consultants who have previously been involved in public sector projects) were used. In all, the pilot study participants were 8 male and 2 females, with the mean age range being 25-34.

To obtain the respondents, a snowball sampling method was employed as a distribution vehicle. KwikSurveys.com was used as the collection method and the responses were exported into SPSS for statistical analysis. To form the hypothesis, theoretical principles of DOI and the published, archival media documents were employed. The principal hypothesis guiding this research is that there is little or diminishing trust in e-government ISS. This is based on the theoretical elements of trialability and compatibility and the practical view that breaches in ISS have taken place in the past year and widely reported in the media. Initially, 500 respondents were contacted, but, due to time and system compatibility constraints, 277 males and 112 females were used. All participants gave consent to take part in the survey and the data was coded for confidentiality. Table 1 illustrates the demographic variables.

Table 1: Demographic variables

Demographic variables		**N=389**
Sex	% male	71.2
Age	Mean Years	25-34
	Range	18 to 24 - 55 to 64
Qualifications %	No qualifications	7.2
	GCSE or equivalent	14.9
	A-level or equivalent	3.3
	Degree or equivalent	60.7
	Postgraduate or equivalent	13.9
Ethnicity %	Caucasian	70.7
	Mixed	1.0
	Asian or British Asian	24.4
	Black or British Black	2.6
	Chinese or other ethnic group	1.3
Income %	Less than £7500	16.5
	£7500=£13,499	14.4
	£13,500-£24,999	27.2

	£25,000-£49,999	35
	£50,000+	6.9

RESULTS

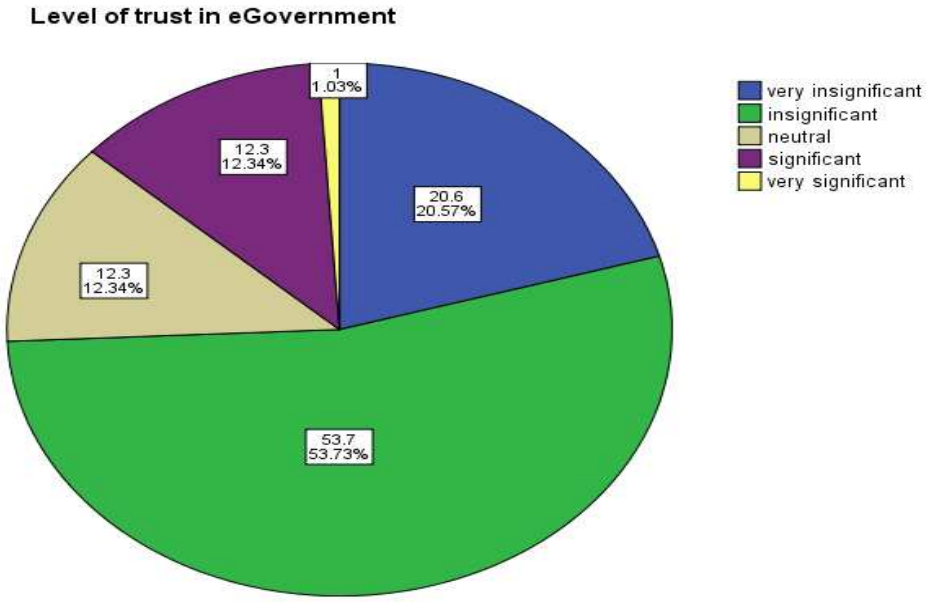
Hypothesis 1

Trust in Government: The lower the level of trust in Government, the lower the disposition to adopt G2C services.

Spearman's correlation indicated a strong correlation between lack of trust in eGovernment and the intention to use eGovernment: $r_s = .36$ (389) $p < 0.01$ (2-tailed). 74.3% of respondents rated trust in eGovernment as insignificant (this percentage was reached by pooling the responses from the 'very insignificant' and 'insignificant' categories) (see figure 1). However a Chi-square test found, that people are still likely to use eGovernment services in the future ($X^2 = 150.67$, df = 16, $p = 0.01$).

This suggests that trust in eGovernment is not a barrier against the intention to use eGovernment services. Although people felt that trust in eGovernment is important, they were also influenced by convenience and privacy when measured against the intention to use eGovernment. 55 % of respondents were more concerned with convenience as opposed to privacy when choosing to use the internet. At the same time, it was felt that trust in eGovernment is important. From this result it can be argued that convenience is a more important adoption factor in that it overrides the decision to (or not to trust) online Government.

Figure 1: Response distribution to level of trust in eGovernment



Hypothesis 2

Information security awareness: The higher the level of information security awareness, the higher the disposition to adopt G2C services.

No correlation was found between information security awareness and the intention to use eGovernment services. Table 2 below illustrates a trend towards the likelihood of intending to use eGovernment services associated with knowing what the gold padlock and https[5] icons illustrate on some websites.

Table 2: Information security awareness

[5] The padlock and https were selected as security measures as those are widely publicised in the media when security is emphasised.

		Do you intend to use online Government services in the future?					
		very unlikely	unlikely	neutral	likely	very likely	Total
Do you know what HTTPS means?	NO	8	12	18	112	25	175
	YES	11	15	14	134	40	214
Total		**19**	**27**	**32**	**246**	**65**	**389**
Do you know what the gold padlock symbol illustrates on some websites?	NO	5	5	9	53	11	83
	YES	14	22	23	193	54	306
Total		**19**	**27**	**32**	**246**	**65**	**389**

Hypothesis 3

Privacy Concerns: The higher the privacy concern, the lower the predisposition to adopt G2C services.

The concern for privacy was significantly correlated with the intention to use eGovernment. Those agreeing that the Government is keeping their information safe are more likely to use eGovernment services in the future: (X^2 = 259.75, df = 16, p = 0.001). Those concerned with privacy were significantly less likely to intend to use eGovernment services than those whose concern was convenience: (X^2 = 121.33, df = 4, p = 0.001). This is in agreement with results that found those who were less concerned about their online privacy were still likely to use eGovernment services in the future: (X^2 = 320.34, df = 16, p = 0.001).

DISCUSSION

The results of this research revealed that age and level of education are significant factors with younger and more educated citizens more likely to use eGovernment services. This is in accordance to previous studies that merited younger and more educated individuals as markers for adoption (Choudrie and Grey, 2008; Dwivedi and Williams, 2008) and indicates digital divide to be a contentious issue. These factors are also correlated to: higher levels of internet experience skills, spending more hours online and a better awareness of information security and privacy. The findings also found the majority of respondents to be concerned (to varying degrees) with privacy and security of their information when using eGovernment services. The results are not surprising given the bulk of respondents were from the demographics most likely to adopt eGovernment. Also, citizens may be sceptical and mistrust eGovernment initiatives believing they may result in an invasion of privacy studies (James: 2000; Norris & Moon: 2005; Dutton and Shephard; 2006). These studies also found a major barrier to eGovernment adoption as being issues related to security, lack of technology or web experience and issues regarding privacy. Given the majority of respondents were highly skilled and ISS aware, the respondents positively favoured eGovernment adoption despite mistrusting eGovernment.

With respondents trusting the internet (including e-commerce) more than eGovernment; it appears that while citizens distrust eGovernment, they are still more likely to use online services than not. This is a result of more citizens favouring convenience over privacy when deciding to use an online service (as indicated in the findings for hypothesis 3). This appears to be in conflict with previous studies that stated public trust in eGovernment is a primary input of transactional usage (Belanger et al: 2002; Dutton & Shephard: 2006; Beynon-Davies: 2007; Park: 2008). This can be attributed to having a more educated and experienced sample of participants (being adoption sensitive as opposed to adoption averse). This indicates the gap between G2C and e-commerce perceptions to be closing (for the adoption sensitive demographic) and can be partially explained by the Government's channel strategy of delivering eGovernment services by emulating the private sector's approach towards focusing on the customer (citizen centric service delivery) (Cabinet Office: 2007; NAO: 2007).

Yet, this appears to be in contention (but not with the inexperienced users who are still in concordance to the studies) with the opinions signposted on other studies (Griffin & Halpin: 2005; Parent: 2005) claiming the lack of stakeholder involvement was a major barrier. An attribution between the majority of the demographic (and their adoption sensitive behaviour) and their bias towards convenience could explain this finding. The decision to adopt eGovernment for convenience over privacy is further enhanced by the majority of citizens who significantly associated the decision to adopt eGovernment services to the perceived usefulness (relative advantage) of eGovernment, a view supported in other studies (Agarwal and Prasad: 1998; Carter and Weerakkody: 2008).

CONCLUSION

The aim of this paper is to explore how the UK is dealing with the issues of security, privacy and trust when adopting and using online government products or services. The UK eGovernment agenda does not appear to be in conflict with the privacy and security requirements of citizens. The Government does appear to have implemented a secure delivery platform, albeit one that requires better leadership and governance. While ISS does not appear to be a broader adoption issue at the moment, the ongoing security breaches may alter citizen's perceptions, potentially alienating those planning to use G2C eGovernment in the future (out of convenience more so than any other factor; but demographics, trust, convenience, internet experience and perceived usefulness are factors that have been identified as adoption enablers).Improvements to the IAG strategy could include the increased use of e-commerce best practices, bringing proven and familiar secure electronic delivery methods to UK citizens who are well versed with the online marketplace (as indicated in the findings citizens trusted e-commerce more than eGovernment, but this gap is closing as a result of the Governments citizen centred approach).

The limitations of this research includes a disproportionate representation of the UK demographic; with the majority of the sample being young, well educated citizens and 30% of the sample being of ethnic origin (Asian or British Asian). Further limitations include the lack of input from those involved in eGovernment projects that could have made a valuable contribution in balancing the opinions of citizens to produce a more holistic study. Furthermore the sample size was relatively small for a survey and that future work should aim to increase the sample size. Surveys tend not to explore the reasoning and perspective's of respondents very well; thus using focus groups and interviews to supplement the survey would have generated better opinions.

Future directions for this research include, analysing the relationship between eGovernment adoption and other nationwide technological adoption decisions that citizens have to make; the adoption of broadband being one example. Also future research should combine both quantitative and qualitative approaches to validate responses and provide depth, thereby helping understand the citizen perspective in greater detail.

REFERENCES

Agarwal, R., & Prasad, J. (1998). The antecedents and consequents of user perceptions in e-government information technology adoption. *Decision Support Systems*, 22(1), pp.5–29.

Barriers to Adoption Report (2007. Available at http://www.egovbarriers.org/?view=resources Last accessed 20th August 2008.

Bélanger, F. & Hiller, J. (2005) A framework for e-government: Privacy implications. *Business Process Management Journal*, 11.

Beynon-Davies, P. (2007). Models for e-government. *Transforming Government: People, Process and Policy*. 1 (1), pp.7.

Cabinet Office (2007). Central Sponsor for Information Assurance: A National Information Assurance Strategy. Cabinet Office, London.

Cabinet Office (2008). Transformational Government Annual Report. Cabinet Office, London.

Carter, L. & Weerakkody, V. (2008) E-government adoption: A cultural comparison. *Information systems frontiers.* 10 (4) pp.473.

Carter, L. and Belanger, F. (2005) "The utilization of e-government services: citizen trust innovation and acceptance factors". *Information Systems Journal*, 15 (1), pp.5-25.

Choudrie, J., Grey, S. and Tsitsianis, N. (2008). EVALUATING THE DIGITAL DIVIDE: THE SILVER SURFER'S PERSPECTIVE. Pre-ICIS [Sig on Dev] Workshop

Choudrie, J., Brinkman, Paul-W., and Pathania, R. (2007). Using Diffusion Theory to determine the Digital Divide in E-Services; Two UK Local Area Perspectives. *Electric Government: An International Journal,* 4, **3**, pp. 345-59.

Dourish, P. & Anderson, K. (2006). Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction, 21*(3), pp.319-342.

Dutton, W., & Shepherd, A. (2006). Trust in the Internet as an experience technology. *Information, Communication & Society*, 4(9), pp.433–451.

Dwivedi, Y. & Williams, M. (2008) Demographic influence on UK citizens' e-government adoption. *Electronic Government, an International Journal.* 3 (5). pp.261.

Egan, M. & Mathen, T. (2005) *The executive guide to information security: threats, challenges, and solutions*. 1st edn. Addison-Wesley, Indianapolis.

Elliman, T., Irani, Z., Jackson, P. (2007) Establishing a framework for eGovernment research: project VIEGO. *Transforming Government: People, Process and Policy,* 1 (4), pp.64–376.

Gilbert, D., Balestrini, P., & Littleboy, L. (2004). Barriers and benefits in the adoption of e-government. The International Journal of Public Sector Management, 17(4/5), 286–301.

Griffin, D. and Halpin, E. (2005). An Exploratory Evaluation of UK Local e-Government From an Accountability Perspective. *The Electronic Journal of e-Government*. 3, (1):13-28.

Irani, Z. , Love, P.E..D., Elliman, T., Jones, S. & Themistecleous, M. (2005). Evaluating eGovernment: learning from the experiences of two UK local authorities. *Information Systems Journal*. (15): 61-82.

James, G. (2000). Empowering bureaucrats. *MC Technology Marketing Intelligence.* 20 (12) pp.62-8.

Jorgensen, D. J. and Cable, S. (2002). Facing the Challenges of E-Government: A Case Study of the City of Corpus Christi, Texas. SAM Advanced Management Journal, 67, **3**:15-21.

Mason, S. & Hacker, K. (2003) Applying communication theory to digital divide research. *IT & Society* 1 (5) pp.40–55.

Mirchandani, D. A. et al. 2008, Perspectives of citizens towards e-government in Thailand and Indonesia: A multigroup analysis. *Information systems frontiers,* 10 (4), pp.483

(NAO) National Audit Office Annual Report (2007)

Norris, D. & Moon, M. (2005). Advancing E-Government at the Grassroots: Tortoise or Hare? *Public Administration Review* 65(1) pp. 64-74.

Parent, M. (2005) Building citizen trust through e-government *Government Information Quarterly* 22, pp. 720–736.

Park, R. (2008). Measuring Factors that Influence the Success of E-Government Initiatives. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences.* (HICSS 2008)

Prins, C. (2001) *Designing eGovernment: On the crossroads of technological innovation and institutional change.* 1st ed. The Hague: Kluwer Law International.

PWC (2006) Information Security Breaches Survey 2006 Technical Report, available at: http://www.pwc.com/extweb/pwcpublications.nsf/docid/7FA80D2B30A116D7802570B9005C3D16

Rogers, E.M. (1995), *Diffusions of Innovations*, 4th ed., Free Press, New York, NY.

Saltzer, J. H. & Schroeder, M. D. (1975) The protection of information in computer systems. *Proceedings of the IEEE*, **63**(9), pp. 1278–1308.

Silcock, R. (2001) What is e-Government? *Parliamentary Affairs*, 54, pp.88-101.

Smith, S. & Jamieson, R. (2006) Determining Key Factors in E-Government Information Systems Security. *Information Systems Management*, 23 (2), pp.23-32.

Thibodeau, P. (2000) E-government spending to soar through 2005. *Computerworld.* 34 (17) pp. 12.

Tornatzky, L. & Klein, K. (1982) Innovation characteristics and innovation adoption implementation: a meta-analysis of findings. *IEEE Transactions on Engineering Management* (29) pp. 28–45.

Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis (2003). User Acceptance of Information Technology: Toward a Unified View. MISQ, 27, 3:

Wood, D., (2006). *A report on the surveillance society.* Report for Information.