Βιβλιογραφία για Διαχείριση Ταυτότητας και Ηλεκτρονική Διακυβέρνηση

'Εκδοση 01

Abie, H., B. Foyn, et al. (2004). "The need for a digital rights management framework for the next generation of e-government services." Electronic Government 1(1): 8-28.

The amount of goverment information is huge and relies mostly on traditional systems, inaccessible to citizens and often to government departments. In today's digital era, most of this content can be more intelligently processed and intergrated within e-government. In the world of the future, where ambient intelligence and e-governments are a reality, citizens will interact with the available services in all areas of their lives; a situation that presents new challenges in the area of Digital Rights Management (DRM). Taking into account the nature of the information amd the needs of different governmental departments and citizens, any e-government research must give full attention to DRM. In the process towards successful e-government, properly handling privacy, security and trust is an indispensable precondition for reliable legal safeguards, reliable technology and secure business, and for achieving acceptance by citizens. Therefore, we propose to establish a Network of Excellence (NoE) for a framework for policy, privacy, security, trust and risk management for DRM. The NoE will consist of experts from various disciplines and will conduct and guide on-going and future high quality research on e-government related domains.

Agentcities (2003). Harmonising heterogeneous security models using an ontological approach: 1-22.

There is a plethora of different security standards proposed by a range of standards consortia including the IETF, W3C and OASIS. In a heterogeneous open service environment, the variety of security standards used can hinder security interoperability because a common security configuration can't always be agreed in advance, discovered dynamically or reconfigured dynamically. In this report, we have developed a generic security model expressed in an XML extension (DAML) and have investigated how to ground this in order to reuse the security specifications from the W3C etc. We have undertaken some initial work in order to apply this model to support security configuration discovery and personal privacy. This report is organized as follows. In Section 1 we expand upon the motivation for our security model, then the objectives and milestones of the report are given in Section 2 and some existing security models and specifications are surveyed in Section 3. Our common ontological model is proposed in Section 4 where it is divided into the core conceptual layer in Section 4.1, and the remaining layers with an outline on how we can apply the model to support the discovery of security configurations in Section 4.2. Subsequently, this is followed by some preliminary work on how to extend these models to support personal privacy in Section 5.

Agre, P. E. and C. A. Harbs (1994). "Social choice about privacy: Intelligent vehicle-highway systems in the United States." Information Technology & People 7(4): 63-90.

Broad coalitions of companies, governments, and research institutions in several countries are currently designing massive electronic infrastructures for their roadways. Known collectively as intelligent vehicle-highway systems (IVHS), these technologies are intended to ease toll collection and commercial vehicle regulation, provide drivers with route and traffic information, improve safety and ultimately support fully automated vehicles. Although many aspects of IVHS are uncertain, some proposed designs require the system to collect vast amounts of data on individuals' travel patterns, thus raising the potential for severe invasions of privacy. To make social choices about IVHS, it is necessary to reason about potentials for authoritarian uses of an IVHS infrastructure in the hypothetical future. Yet such reasoning is difficult, often veering towards Utopian or dystopian extremes. To help anchor the privacy debate, places IVHS privacy concerns in an institutional context, offering conceptual frameworks to discuss the potential interactions between IVHS technologies and the computer design profession, standards-setting bodies, marketing organizations, the legal system and government administrative agencies.

Al-Qirim, N. (2004). Strategic ehealth planning In healthcare organisations in New Zealand: A telemedicine perspective. 17th Bled eCommerce Conference: eGlobal, Bled, Slovenia.

This research reviewed the health IS (HIS) strategy of the New Zealand government and highlighted different gaps in this strategy, as raised by the different stakeholders involved in this strategy. In order to address such gaps, the government provided different Critical Success Factors (CSFs) for the successful implementation of the national HIS strategy. This research introduced the telemedicine technology, as one of the solutions for the HIS strategy with an objective to deliver integrated healthcare services to rural communities specifically. The research assessed the strategic importance of telemedicine by highlighting its Strengths, Weaknesses, Opportunities and Threats (SWOT) to healthcare providers. The research utilised the portrayed HIS strategy and the CSFs to portray a strategy for telemedicine integration in New Zealand taking into consideration its SWOT. The developed CSFs are of strategic importance to healthcare professionals, researchers and policymakers interested in integrating telemedicine in healthcare delivery at the national level in New Zealand and elsewhere.

Alge, B. J. (2001). "Effects of computer surveillance on perceptions of privacy and procedural justice." Journal of Applied Psychology 86(4): 797-804.

Electronic workplace surveillance is raising concerns about privacy and fairness. Integrating research on electronic performance monitoring, procedural justice, and organizational privacy, the author proposes a framework for understanding reactions to technologies used to monitor and control employees. To test the framework's plausibility, temporary workers performed computer/Web-based tasks under varying levels of computer surveillance. Results indicated that monitoring job-relevant activities (relevance) and affording those who were monitored input into the process (participation) reduced invasion of privacy and enhanced procedural justice. Moreover, invasion of privacy fully mediated the effect of relevance and partially mediated the effect of participation on procedural justice. The findings are encouraging for integrating theory and research on procedural justice and organizational privacy.

Alvesson, M. and H. Willmott (2001). Identity regulation as organizational control: Producing the appropriate individual. Institute of Economic Research Working Paper Series. S. o. E. a. Management. Lund, Lund University: 32.

This paper takes the regulation of identity as a focus for examining organizational control. It considers how employees are enjoined to develop self-images and work orientations that are deemed congruent with managerially defined objectives. This focus on identity extends and deepens themes developed within other analyses of normative control. Empirical materials are deployed to illustrate how managerial intervention
operates, more or less intentionally and in/effectively, to influence employees' self -constructions in terms of coherence, distinctiveness and commitment. The processual nature of such control is emphasized, arguing that it exists in tension with other intra and extra-organizational claims upon employees' sense of identity in a way that can open a space for forms of micro-emancipation.

Andersen, K. V. (1998). EDI and data networking in the public sector, Kluwer Academic Publishers.

Andersen, K. V., H. Z. Henriksen, et al. (2004). Stray dogs and wild cats tracking down information systems in government? European Conference of Information Systems, Turku, Finland.

This paper explores the body of e-government research surfaced during 1998-2003 in Web of Science and ProQuest. The search identified 158 scholarly papers. Using a classification model developed by Andersen and Danziger (1995), the predominately part of the research addresses improvements of services and products (72%), better data access (67%) and public-Government interaction (64%). Less frequent are studies on values. Comparing data with literature review on the Golden Age of transformation of the public sector (1988-2000), the authors suggest that e-government so far has not altered the balance between existing domains of applications or introduced new areas.

Andersen, K. V. and N. C. Juul (2003). User democracy and digital channels. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

This paper evaluates the formal digital access channels for exercising involvement of the users in the governance of local governmental institutions. The paper is based on an analysis of web-based channels for user and citizen involvement in decision-making processes within the areas of eldercare, childcare, schools, and municipality councils. Rather than painting an idyllic picture of citizen digital access to information and interaction, our analysis of three Danish municipalities suggests that the public sector has made no or very limited digital progress along the governance avenue.

Andersen, K. V. and N. C. Juul (2004). Digital wheel barrows In local government. 17th Bled eCommerce Conference: eGlobal, Bled, Slovenia.

This paper finds through a vertical and horizontal study of local municipalities and health data network, that government has excelled in acquiring and re-using data in a digital format. The continuously and successful reliance on transaction and process improvements is contrasted by no or only marginal use of data to improve the core of services. The study suggests that most data are available in the least end-user oriented processes and that government appears to be reinforcing, rather than leveling, this imbalance.

Arcieri, F., G. Melideo, et al. (2002). "A reference architecture for the certification of e-services in a digital government infrastructure." Distributed and Parallel Databases 12(2): 217-234.

Certifying the execution of a service is a critical issue for an e-government infrastructure. In fact being able to document that an e-service was actually carried out, given the legal value that is often attached to data managed and exchanged by public administrations, is of the utmost importance. This is made more complex in cases, like it often happens in the public administration sector, where e-services are based on legacy systems managed by autonomous and independent organizations. In this paper we discuss the introduction, within the standard three tier architecture for e-services, of an architectural subsystem providing certification functions. This architecture features both physical and functional independence from the application level and is made up by new control components providing a highly efficient solution for certification requirements. Our solution has been successfully tested in real-world systems developed in Italy to support digital government functions

Argyriades, D. (2003). "Values for public service: Lessons learned from recent trends and the Millennium Summit." International Review of Administrative Sciences 69(4): 521-533.

This article was originally prepared for circulation at the Second Specialized International Conference of the IIAS, which took place in New Delhi from 5 to 9
November 2002. It was presented orally, in a much abridged form, in the context of the Workshop on Relations between International Organizations and National Administrations in Sustainable Development Policies. As the title suggests, the article's point of departure is the Millennium Summit (September 2000) and the sequence of events which have followed and are still unfolding. The Millennium
Declaration and the logic of the events of the past two years bring into sharp relief the salience of good governance and of public service values, in this context. They also, one could argue, cast doubt on the validity of managerial doctrines which held sway in
the 1980s and 1990s and undermined these values. The market model of government assiduously pursued the shrinkage of the state and the devaluation of public service. It questioned the identity of public administration and promoted the idea that governments should follow and adopt not only the methods and practices but also the values of business. Efficiency and effectiveness ranked at the top of those values. Regulations and rules were discounted. 'Results' were enjoined over 'process'.
In retrospect, the outcomes of this approach have proved very uneven and mixed. Experience demonstrates the need for some degree of separation between the world of business and that of government, between the private sector and the public sphere.
Some boundaries are necessary in order to emphasize their separate identities, enhance
public service professionalism, reinforce a public service ethic and restore public trust in government. More than anything else, a degree of separation is needed to preserve and to sustain integrity, commitment, objectivity and independence, which must be seen as the marks of the true professional.

Ashley, P. (2002). E-P3P privacy policies and privacy authorization. The 2002 ACM workshop on Privacy in the Electronic Society, Washington, DC.

Enterprises collect large amounts of personal data from their customers.To ease privacy concerns,enterprises publish privacy statements that outline how data is used and shared. The Platform for Enterprise Privacy Practices (E-P3P)defines a fine-grained privacy policy model.A Chief Privacy Officer can use E-P3P to formalize the desired enterprise-
internal handling of collected data.A particular data user is then allowed to use certain collected data for a given purpose if and only if the E-P3P authorization engine allows this request based on the applicable E-P3P policy. By enforcing such formalized privacy practices, E-P3P enables enterprises to keep their promises and prevent accidental privacy viola-
tions.

Auerbach, N. (2003). Smart card support for anonymous citizen services. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

Numerous European countries are currently engaging in e-government initiatives that often comprise issuing digital identification cards to citizens. As most of these cards base access control solely on the identity of the cardholder, the issue of privacy arises. We present a scenario where it is desirable that citizens can access services while remaining fully anonymous. We consider the requirements for an anonymous access from the perspective of both government and citizens. Starting from the idea of mapping the problem of anonymous access to a group membership problem we present a credential-based solution in which digital credentials are used to extend the digital identity of the citizen. We consider the infrastructural components that an administrative body must introduce when using credentials for service access. We finally propose cryptographic means for the implementation of such a system with low-cost cryptographic credentials and smart cards. The implications of the smart card as a computationally restricted environment are discussed and an outlook on future research on credentials in e-government use is given.

Backhouse, J. (2002). "Assessing certification authorities: Guarding the guardians of secure e-commerce?" Journal of Financial Crime 9(3): 217-226.

E-commerce, Public Key Infrastructure (PKI), interoperability, legal and regulatory issues related to PKI interoperability, International Standards, cross-certification, Cross-recognition via accreditation schemes, CA accreditation schemes, Actors in the CA accreditation framework, Using PKI assessment schemes (scope, system security, operations, supervisory regime, personnel, disclosures)

Bacon, J., K. Moody, et al. (2003). "Access control and trust in the use of widely distributed services." Software: Practice and Experience 33(4): 375 - 394.

OASIS is a role-based access control (RBAC) architecture for achieving secure interoperation of independently managed services in an open, distributed environment. OASIS differs from other RBAC schemes in a number of ways: role management is decentralized, roles are parametrized, roles are activated within sessions and privileges are not delegated. OASIS depends on an active middleware platform to notify services of any relevant changes in their environment.
Services define roles and establish formally specified policy for role activation and service use (authorization); users must present the required credentials and satisfy specified constraints in order to activate a role or invoke a service. The membership rule of a role indicates which of the role activation conditions must remain true while the role is active. A role is deactivated immediately if any of the conditions of the membership rule associated with its activation become false.
OASIS introduces the notion of appointment, whereby being active in certain roles carries the privilege of issuing appointment certificates to other users. Appointment certificates capture the notion of long-lived credentials such as academic and professional qualification or membership of an organization. The role activation conditions of a service may include appointment certificates, prerequisite roles and environmental constraints.
The role activation and authorization policies of services within an administrative domain need not embody role hierarchies nor enforce privilege delegation. But OASIS is sufficiently flexible to capture such notions, through prerequisite roles and appointments, if they are required within an application domain.

We define the model and architecture and discuss engineering details, including security issues. We illustrate how an OASIS session can span multiple domains and we propose a minimal infrastructure to enable widely distributed, independently developed services to enter into agreements to respect each other's credentials. In a multi-domain system access control policy may come from multiple sources and must be expressed, enforced and managed. In order to respond to changing relationships between organizations it should be easy to allow role holders in one domain to obtain privileges in another. Our approach to policy and meta-policy management is described.
We speculate on a further extension to mutually unknown, and therefore untrusted, parties. Each party will accumulate audit certificates which embody its interaction history and which may form the basis of a web of trust.

Baier, T., C. Zirpins, et al. (2003). Digital identity: How to be someone on the net. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

Personal communication and collaboration has been and still is a major driver of the Internet. A severe drawback in human centric electronic interaction is the fuzziness of the image that the co-operation partners have of each other (i.e. their respective "identities") – especially in different and varying application contexts. This uncertainty adversely affects increasingly important "soft" co-operation factors like, e.g., trust and social behavior, and should therefore be minimized whenever possible. In addition, the lack of a homogenous representation of digital identities results, even at the system level, in many cases in increased and unnecessary administration tasks – like, e.g., keeping track on user-ids and passwords or typing the same information several times. This makes communication inefficient and error-prone and may introduce various privacy threats. On the other hand, neither the minimal identity representation which is already used at the system's level (e.g. a user-id used for security reasons), nor the emerging proprietary efforts for identifying users uniquely at the application level (e.g. for "single sign on" purposes) suffice for comprising the user's identity fully as needed for co-operation of individual human beings.
In order to cope with such problems of proper electronic user "identification", we propose an open and generic notion of a digital identity that is generally applicable and includes an extensible set of identity facets on the system- as well as the user-level. Such a unique digital identity for all possible Internet communication and co-operation tasks enables users to recognize distinct co-operation partners uniquely in many different contexts – but also allows for revealing individual (i.e. only partial) views on such information whenever necessary. Therefore, such a facility enriches communication by semantic information about co-operation partners and thus enables faster, more secure and trustworthy collaboration. In summary, this paper proposes the concept of a digital identity and specifies what challenges are to be met when building an open, distributed, decentralized system infrastructure for digital identities.

Banerjee, P. and P. Y. K. Chau (2004). "An evaluative framework for analysing e-government convergence capability in developing countries." Electronic Government 1(1): 29-48.

The e-government objectives of a country go well beyond providing constituents with government information and services by leveraging information and communication technology. Although it is a crucial step, the desired goal is that of convergence characterised by ubiquitous access to government information and services and total transparency of government functioning, a stage that contributes to the social and economic wellbeing of citizens. Some developed countries are already engaged in the transformation of the governance process through increased citizen participation and are attempting to create an open, transparent environment through convergence of information and services. However, developing economies, especially poor ones, lag far behind their more prograssive counterparts. Based on prior literature, this study proposes an evaluative framework for analysing e-government convergence capability in developing countries and applies it to analyse the prospects of convergence in a few selected developing countries. The results indicate that the quality and range of government information and services vary significantly across the countries, attributed in some measure to the e-leadership capability of the countries. However, we argue that e-leadership may not be able to readily combat social maladies, such as low literacy and awareness education - required for the meaningful use of information and interaction, or economic handicaps, such as living standards that impact on the citizen's ability to procure web-based access; these factors being crucial for e-government convergence.

Barca, C. and A. Cordella (2004). Seconds out, round two: Contextualising egovernment projects within their institutional milieu - A London local authority case study. European Conference of Information Systems, Turku, Finland.

It is early days yet to be able to truly determine whether the visions of e-government are realisable or not. The focus of the majority of the projects, and even research, on e-government has been on the possible impact of technology on government's interaction with citizens. This paper looks beyond this level, investigating the challenges faced by local government authorities when implementing egovernment projects. A case study within a forward looking London borough implementing an eprocurement system was carried out. The research data suggests that the uncertainties faced by the authority during the implementation, and the mechanisms enforced to tackle them, have to be considered if we want to better understand the chances of success of e-government projects. The study hints that amongst these uncertainties the institutional barrier of departmentalism, which lies deep in the public sector, is playing a major role in defining the possible outcome of e-government projects. The paper concludes that this organisational barrier has to be undoubtedly considered to comprehend the chances of ICT driven reforms such as public sector e-procurement.

Barnum, G. (2002). "Availability, access, authenticity, and persistence: Creating the environment for permanent public access to electronic government information." Government Information Quarterly 19(1): 37-43.

Barreto, M. and N. Ellemers (2002). "The impact of respect versus neglect of self-identities on identification and group loyalty." Personality and Social Psychology Bulletin 28(5): 629-639.

How do targets deal with a discrepancy between their choice of identity and the way they are categorized by others?In this article, the authors demonstrate that participants reactions to this discrepancy depend on whether the way they are actually treated by others respects their chosen identity.Participants whose choice of identity was neglected expressed low identification and little loyalty to the group to which they had been assigned. By contrast, identification and group loyalty were stronger among participants whose choice of identity was respected and who did not dif-
fer from controls on these measures.Of importance,only participants whose self-identity was respected also were willing to self-categorize in and express willingness to cooperate with the ascribed group.The implications of these results for the under-
standing of identity processes in pluralist societies are discussed.

Basden, A., E. Ball, et al. (2001). "Knowledge issues raised in modeling trust in a public key infrastructure." Expert Systems 18(5): 233-249.

The paper describes a knowledge-based system for modeling trust in the certification authority (CA) of a public key infrastructure. It was built using a graphical knowledge-based system toolkit, Istar, that allows the knowledge builder to easily model the important relationships between concepts of the domain. The knowledge base was initially built using published work and was subsequently extended by knowledge obtained from leading public key infrastructure experts. The first prototype system computes the trust in a CA by asking the user a series of questions about the CA's Certification Practice Statement. Examples of its use with two well-known public CAs is discussed.
An important issue raised and discussed in this paper is how to map symbols in the knowledge base to the knowledge level of human trust and beliefs, for such an ill-defined area of knowledge as trust, and four main mappings have been identified. Another issue that emerged relates to the use of questionnaires during knowledge acquisition. The expert system is currently available online via the Istar knowledge server, and future work is discussed.

Beynon-Davies, P. (2004). Constructing electonic governement: The case of the UK Inland Revenue. European Conference of Information Systems, Turku, Finland.

The term electronic government (e-Government) generally refers to the use of information and communications technology (ICT) to change the structures and processes of government organisations. Many governments world-wide have invested heavily in this agenda but there is a lack

of clear case material which describes the potentialities and pitfalls experienced by organisations at the forefront of this change. The department of the Inland Revenue has been at the forefront of this electronic government e-Government vision in the UK. The department has undertaken major attempts to re-engineer its interface with the UK citizen and other stakeholders. It has also suffered a number of highly publicised failures in delivering its services electronically. This paper presents a case study of the process of 'constructing' e-Government experienced by this organisation. We place this organisation's attempts at ICT innovation within the context for e-Government within the UK. We also use a model developed as part of our research - the electronic government organisation - to help explain some of the potentialities and pitfalls in this area. In terms of this analysis we review definitions of e-government and call for a more holistic use of the term in the development of future strategy.

Bimber, B. (1999). "The Internet and citizen communication with government: Does the medium matter?" Political Communication 16(4): 409-428.

N\A

Bodorik, P. and D. Jutla (2003). Architecture for user controlled privacy. Proceedings of the 2003 ACM symposium on Applied computing.

Empowering users to make informed decision-making over online release of private data is a challenge in today's society. A large majority of users has rejected many e privacy business models including Lumeria's,Zero Knowledge and Microsoft 's PassPort. In detailing privacy requirements for an architecture for user-controlled e privacy, we provide some key reasons, mainly centered around user's perception of control, behind the apparent dismissal of business models for privacy based on trusted platform, that supports privacy requirements for enhanced user control of privacy. Privacy management issues that are addressed include the identification of data repositories and their purposes, users agents and their role and interactions, and the separation of persona profile information from user preference information.

Bongers, F., C. Holland, et al. (2003). Measuring e-government. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

In this paper we describe research we have conducted on measuring e-government in the Netherlands. This research was commissioned by the Ministry of Economic Affairs and the Ministry of the Interior in the Netherlands. There are many aspects and benefits of e-government which are missing in existing measuring tools and concepts. Existing benchmark studies lack a theoretical basis and merely look at the availability of electronic government services. Actual use or the impact of electronic public services is not captured. We therefore have developed a new concept and measuring tool on egovernment. This tool is being used in our benchmarking study. We have described methodological aspects of our approach in this paper. We believe our experience in this research project and this measuring tool can contribute to the discussion on new ways to measure and evaluate e-government in an international perspective.

Boufeas, G., I. Halaris, et al. (2004). Business plans for the development of e-government in Greece: An appraisal. UNTC Occasional Papers Series. T. Tsekos. Thessaloniki, United Nations Thessaloniki Center for Public Service Professionalism.

Brockner, J. (2002). "Making sense of procedural fairness: How high procedural fairness can reduce or heighten the influence of outcome favorably." Academy of Management Review 27(1): 58-76.

The interactive effects of procedural fairness and outcome favorability on people's reactions to organizational decisions are considered. When the dependent variable consists of employees' support for decisions, for decision makers, or for organizations, outcome favorability has less influence when procedural fairness is high rather than low. When the dependent variable consists of employees' self-evaluations, however, outcome favorability has more influence when procedural fairness is high rather than low.

Brown, G. (2004). "The use of hardware tokens for identity management." Information Security Technical Report 9(1): 22-25.

Contrasts smart cards with time and event-based tokens for identity management. Considers security requirements of the systems. Draws attention to an issue with the key generation process for the most popular token on the market.

Brunsson, N. and K. Sahlin-Andersson (2000). "Constructing organizations: The example of public sector reform." Organization Studies 21(4): 721-746.

Organisations are socially constructing phenomena. A crucial task for organisational research is to analyze how and why people construct organisations rather than other social forms. In this paper, it is argued that recent public-sector reforms can be interpreted as attempts at constructing organisations. Public-sector entities that could formerly be described as agents or arenas have been transformed into "more complete" organisations by installing or reinforcing local identity, hierarchy and rationality. This interpretation helps to explain important aspects of the reform process.

Buell, D. A. and R. Sandhu (2003). Identity management. IEEE Internet Computing. 7: 26-28.

Byrom, J. and D. Medway (2004). "Cyber solutions to remote problems? Online trading in British overseas territories - A review and research agenda." The International Review of Retail, Distribution and Consumer Research 14(1): 71- 82.

Cairns, G., G. Wright, et al. (2002). "Exploring e-government futures through the application of scenario planning." Technological Forecasting & Social Change 71(3): 217-238.

In this paper, we examine the impact of information and communications technologies (ICT) on government departments/agencies and the contribution of external agents to change and development programs. We present empirical evidence of externally facilitated change to mindsets and patterns of behavior within local government through use of a scenario planning-based approach. Our aim was to facilitate the organizational actors' conduct of investigation of the 'limits of the possible' for a range of plausible futures and determination of strategic responses to these. Participants used their own current knowledge and understanding as a basis for development, with the introduction of external 'expertise' to challenge their thinking and to expand their understanding. Following this, we facilitated the participants' elucidation of key uncertainties on the future, exploration of the relationships between them and possible outcomes. The participants then constructed scenarios that outlined four possible and plausible futures. These held explicit meaning for the participants, enabled them to identify implications of each possible future in relation to structure and service requirements and informed analysis of current structure, service, etc. We compare and contrast the process and outcomes of our scenario-planning intervention (based on intuitive logics) with both those of other futures methodologies (decision analysis, Delphi and environmental scanning) and with other scenario methodologies (trend-impact analysis and cross-impact analysis). We argue that the external facilitation of internal generation of knowledge, understanding and meaning, and of exploration of the limits of the possible for the future, is a valuable tool for comprehending strategic choices. We conclude that our scenario approach, utilizing intuitive logics, enables organizational actors to make sense of the complexities and ambiguities that they face and so facilitates strategic change.

Carey, S. (2002). "Undivided loyalties. Is national identity an obstacle to European integration?" European Union Politics 3: 387–413.

This article posits that national identity is an important element in explaining attitudes towards the European Union. A model of support for European integration is developed that suggests that feelings of national identity are highly important in an individual's choice to support the EU. The impacts of three alternative conceptualizations of national identity are tested. These relate to national identity as an intensity of feelings towards one's country, the level of attachment to the nation and other territorial entities, and the fear of other identities and cultures encroaching on the dominant national culture. The results of ordered logit analyses confirm that stronger feelings of national identity lead to lower levels of support for the EU.

Carlitz, R. D. and R. W. Gunn (2002). "Online rulemaking: A step toward e-governance." Government Information Quarterly 19(4): 389-405.

The adoption of electronic rulemaking by many federal agencies provides an opportunity for a greatly enhanced public role—both in terms of the numbers of people who might participate and the depth of their possible participation. This step towards E-governance poses several challenges for agencies: how they should structure their proceedings, how they can process the comments received and how they can foster and take part in the online communities of interest that will result from this activity. The online tools that may be applied to rulemaking and its ancillary activities—advisory committees, advanced notices of proposed rulemaking and enforcement—can also be used at earlier stages of the legislative process to increase public interest, involvement and commitment. This approach is relevant for all levels of government and for any issue on which public hearings are held or public comment solicited. It can provide an efficient and effective nonadversarial process in which officials and members of the public can mutually define problems and explore alternative solutions.

Castells, M. (2004). The information age: Economy, society, and culture. Oxford, Blackwell Publishers.

Chadwick, A. (2003). "Bringing e-democracy back in." Social Science Computer Review 21(4): 443-455.

The author argues that contemporary digital information communication technologies (ICTs) facilitate new forms of e-government–enabled public sector policy making that enshrine some of the important norms and practices of e-democracy. The potential for linking e-democracy in civil society with e-government at the level of the local and national state is far from straightforward but nevertheless achievable. Following a consideration of the democratization effects of e-democracy and e-government, the author outlines how their norms and practices are converging in four principal areas: online consultations integrating civil societal groups with bureaucracies and legislatures, the internal democratization of the public sector itself, the involvement of users in the design and delivery of public services, and the diffusion of open-source collaboration in public organizations. These now feature as some of the core areas for research in this field and our broader understanding of how ICTs are reshaping governance, the state, and democracy.

Chadwick, A. and C. May (2003). "Interaction between states and citizens in the age of the internet: "e-Government" in the United States, Britain, and the European Union." Governance 16(2): 271-300.

We examine the origins of the recent shift towards "e-government" in three cases: the United States, Britain, and the European Union. We set out three heuristic models of interaction between states and citizens that might underpin the practice of "e-government." Focusing on U.S., British, and European Union initiatives, we undertake a comparative analysis of the evolution of key policy statements on e-government reform in national (and supranational) government. We conclude that the democratic potential of the Internet has been marginalized as a result of the ways in which government use of such technology has been framed since the early 1990s. An executive-driven, "managerial" model of interaction has assumed dominance at the expense of "consultative" and "participatory" possibilities.

Chen, H. (2003). "Digital government: Technologies and practices." Decision Support Systems 34(3): 223-227.

Chen, Y.-C. and J. Perry (2003). "Outsourcing for e-government. Managing for success." Public Performance & Management Review 26(4): 404-421.

This study offers both an analytical framework of and empirical evidence on the key management strategies and capacities for successful information technology (IT) outsourcing by public agencies. The analytical framework draws insights from studies on IT and public administration, public sector contracting out, and business information systems and IT outsourcing. Using the framework, the research examines IT outsourcing at three federal agencies. Data were collected through interviews and document review, which

were analyzed using the variable-oriented comparative case method. In general, this study confirms the importance of management and capacity building in IT outsourcing. Moreover, the results offer specific guidance on IT outsourcing. First, public agencies need to take along-term, strategic approach to managing IT outsourcing arrangements. Second, IT outsourcing should be considered a managed relationship rather than a traditional procurement. Last, the use of performance measurement with a service-level agreement is an important ingredient for successful IT outsourcing.

Clark, E. (2003). "Managing the transformation to e-government: An Australian perspective." Thunderbird International Business Review 45(4): 377 - 397.

Australia is recognized as a leading country in the move to an information economy, and the Australian government has played a pivotal role in this transformation. This commentary outlines some of the key issues confronting Australia as it moves towards its policy goal of achieving e-government. Although governments differ in the pace and nature of reforms required to bring about the transformation to e-government, many of the underlying issues are the same for most governments

Clarke, R. (1988). "Information technology and dataveillance." Communications of the ACM 31(5): 498 - 512.

Data surveillance is now supplanting conventional surveillance techniques. With this trend come new monitoring methods such as personal dataveillance and mass dataveillance that require more effective safeguards and a formal policy framework.

Clarke, R. (1991). "The resistible rise of the national personal data system." Software Law Journal 5(1).

This paper outlines the history of attempts to establish a national personal data system in Australia, with particular reference to the Australia Card proposal and the enhanced Tax File Number scheme. The development of policy measures to deal with information privacy issues is also discussed. The emphasis in revenue collection and benefits administration is moving from reactive enforcement toward proactive data surveillance, and the Privacy Commissioner and privacy interest groups face serious difficulties in their efforts to uphold the social value of information privacy against the increasingly coordinated administrative actions of government agencies.

Clarke, R. (1994). "Human identification in information systems: Management challenges and public policy issues." Information Technology & People 7(4): 6-37.

Many information systems involve data about people. In order reliably to associate data with particular individuals, it is necessary that an effective and efficient identification scheme be established and maintained. There is remarkably little in the information technology literature concerning human identification. Seeks to overcome that deficiency by undertaking a survey of human identity and human identification. Discusses techniques including names, codes, knowledge-based and token-based identification, and biometrics. Identifies the key challenge to management as being to devise a scheme which is practicable and economic, and of sufficiently high integrity to address the risks the organization confronts in its dealings with people. Proposes that much greater use be made of schemes which are designed to afford people anonymity, or which enable them to use multiple identities or pseudonyms, while at the same time protecting the organization's own interest. Describes multi-purpose and inhabitant registration schemes, and notes the recurrence of proposals to implement and extend them. Identifies public policy issues. Of especial concern is the threat to personal privacy that the general-purpose use of an inhabitant registrant scheme represents. Speculates that, where such schemes are pursued energetically, the reaction may be strong enough to threaten the social fabric.

Clarke, R. (1999). Anonymous, pseudonymous and identified transactions: The spectrum of choice. User Identification and Privacy Protection: Applications in Public Administration and E-Commerce, Stockholm.

When designing their information systems, organizations are commonly assumed to be confronted with a stark choice between identification of their clients on the one hand and anonymity on the other.

Identification assures accountability but threatens privacy; whereas anonymity protects privacy but undermines accountability.
This article identifies and explains the spectrum of intermediate alternatives, which involve pseudonymity and varying degrees of authentication. The selection of appropriate alternatives, in most circumstances intermediate between the extremes of identification and anonymity, is argued to be critical to the establishment of trust in electronic commerce, and to the maintenance of social and democratic freedoms.

Clauss, S. and M. Kohntopp (2001). "Identity management and its support of multilateral security." Compute Networks 37(2): 205-219.

We show our approach in developing an identity management system with respect to multilateral security. After examining digital pseudonyms and credentials as basic concepts of such a system, we give an introduction to technologies for multilateral security and describe an architecture which enables multilaterally secure communication. By means of different scenarios we show requirements of an identity management system, and outline an approach in developing an identity manager and its infrastructure. Finally, we discuss problems and risks of identity management systems which must be considered when using such a system.

Coe, A., G. Paquet, et al. (2001). "E-governance and smart communities. A social learning challenge." Social Science Computer Review 19(1): 80-93.

The new information and communications technologies (NICT) and globalization have brought forth a period of great change. Globalization has triggered more intense economic and political interdependencies and has challenged fundamental assumptions about sovereignty and the role of the nation state. As networks increasingly take hold and reshape the way people live, communicate, and work, the question of what kind of governance people will need in the new millennium is raised. Some elements of answers have been put forward under the general rubric of e-governance. It suggests a more community based model of governance with greater connectivity being facilitated by new technology. Application of NICT locally leads to economic, social, and political transformations encapsulated by the new smart community movement. This article provides some preliminary mapping of how the collective intelligence of the communities would operate and how the new governance structures would work.

Commerce, T. N. E. and C. Council (2002). Identity management. NECCC Annual Conference. New York.

Communities, C. o. t. E. (2002). eEurope 2005: An information society for all. t. E. P. Communication from the Commission to the Council, the Economic and Social Committee and the Committee of the Regions. Spain.

Communities, C. o. t. E. (2003). Linking up Europe:The importance of interoperability for e-government services.

Communities, C. o. t. E. (2003). The role of e-government for Europe's future. COM(2003) 567 final. t. E. P. Communication from the Commission to the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels.

Cummings, N. (2004). "Biometric ID technology here to stay." OS Newsletter(June): 18.

Cummings, N. (2004). "Online identity security reaches a crossroads." OR Newsletter(September): 1.

The Electronic Communications Act reached its fourth anniversary in May (25th May to be exact). It was the first Act of the new Millenium. The intention then was that this new Act would transform the future of business and information transactions around the world.

Cummins, G. R. (2003). "Global liability risks emerge in cyberspace." Journal of Internet Law 6(10): 1-11.

Dalpe, R. (2003). "Interaction between public research organizations and industry in biotechnology." Managerial and Decision Economics 24(2-3): 171 - 185.

This paper summarizes the most important findings of the literature on the close interaction between public research organizations and industry in biotechnology. The first question deals with why researchers in academic organizations were and are still important players in the biotechnology industry. Three arguments explain why biotechnology emerged as an organization network: its origins in academic research, the impact of participation in networks on competitiveness and the weight of these networks on R&D intensity and innovation. The second focuses on the factors that explain the regional concentration of such interactions and of biotechnology firms. The paper concludes with a discussion of policy implications. The dynamic of biotechnology is rather unique and can be attributed to the specific institutional arrangements characterizing the American scientific system. Its replication to other sectors or countries seems rather difficult.

Damiani, E., S. De Capitani di Vimercati, et al. (2003). "Managing multiple and dependable identities." IEEE Internet Computing 7(6): 29-37.

Management of multiple and dependable identities is a crucial problem for the development of the next generation of distributed applications. This article illustrates the concept of digital identity management, the motivations for the support of multiplicity and dependability, and provides a discussion on different open issues that need to be addressed toward the support of multiple and dependable identities.

Davidrajuh, R. (2004). "Planning e-government start-up: a case study on e-Sri Lanka." Electronic Government 1(1): 92-106.

This paper analyses the proposed implementation strategies of e-government in Sri Lanka. Firstly, the vision of e-Sri Lanka is presented, that is the information and communication technology development roadmap to achieve e-government. Secondly, a literature study on e-government start-up is given. Also given in the literature study is an approach for analysing implementation strategies; this approach is based on the theory of connection. Thirdly, the proposed implementation strategies are presented and, finally, the strategies are analysed.

Davies, S. G. (1994). "Touching big brother: How biometric technology will fuse flesh and machine." Information Technology & People 7(4): 38-47.

The evolution of information technology is likely to result in intimate interdependence between humans and technology. This fusion has been characterized in popular science fiction as chip implantation. It is, however, more likely to take the form of biometric identification using such technologies as fingerprints, hand geometry and retina scanning. Some applications of biometric identification technology are now cost-effective, reliable and highly accurate. As a result, biometric systems are being developed in many countries for such purposes as social security entitlement, payments, immigration control and election management. Whether or not biometry delivers on its promise of high-quality identification, it will imperil individual autonomy. Widespread application of the technologies would conflict with contemporary values, and result in a class of outcasts.

Dawes, S. S., P. A. Bloniarz, et al. (1999). Some assembly required: Building a digital government for the 21st century. Albany, Center for Technology in Government, University at Albany/SUNY: 39.

Dawes, S. S., V. Gregg, et al. (2004). "Digital government research: Investigations at the crossroads of social and information science." Social Science Computer Review 22(1): 5-10.

Declaration, M. (2003). Como 7-8 July 2003. European eGovernment Conference 2003, Villa Erba Lago di Como.

Deloitte (2002). E-government's next generation: Transforming the government enterprise through customer service. A Deloitte Research Public Sector Study. D. Research, Deloitte Consulting: 41.

Demchenko, Y. (2004). "Virtual organisations in computer grids and identity management." Information Security Technical Report 9(1): 59-76.

This paper provides insight into one of the key concepts of Open Grid Services Architecture (OGSA) Virtual Organisations (VO) and analyses problems related to Identity management in VOs and their possible solution based on using WSFederation and related WS-Security standards. This paper provides basic information about OGSA, OGSA Security Architecture and analyses VO security services. A detailed description is provided for WS-Federation Federated Identity Model and operation of basic services such as Security Token Service or Identity Provider, Attribute and Pseudonym services for typical usage scenarios.

Devadoss, P. R., S. L. Pan, et al. (2003). "Structurational analysis of e-government initiatives: A case study of SCO." Decision Support Systems 34(3): 253-269.

Governments are eagerly looking toward a digital future, but their view is obstructed by the challenges they face in modernizing such vast enterprises. This case study discusses how a government agency developed and implemented an e-procurement system. In particular, the study findings suggest that in the initial stage of any e-government projects, having a tele-cooperation perspective would be useful as it provides a holistic view, focussing on the support of computer-mediated cooperation in a comprehensive sense. We analyse the data using a structurational model, to identify issues in developing this initiative, and construct a framework to analyse future e-government initiatives. We hope to provide a foundation for further discussions on this increasingly important area of research and practice.

Dhillon, G. S. (2001). Social responsibility in the information age: Issues and controversies, Idea Group Publishing.

Doukidis, G., N. Mylonopoulos, et al. (2003). Social and economic transformation in the digital era, Idea Group Publishing.

Drake, D. B., N. A. Steckler, et al. (2004). "Information sharing in and across government agencies: The role and influence of scientist, politician, and bureaucrat subcultures." Social Science Computer Review 22(1): 67-84.

This article is based on an exploratory, interdisciplinary study of issues related to information sharing within and across three public agencies. Based on Schein's work, three subcultures within the public sector (scientist, politician, and bureaucrat) were identified as a framework to examine these issues. Dawes's three categories of benefits and barriers, associated with interagency information sharing (technical, organizational, and political), were also used in developing the framework. Their work has been extended by identifying three types of differences (view, use, and purpose) among these subcultural relationships to data and information. Four types of systems (social, constituency, technical, and organizational) that influence information-sharing processes within and across agencies also were identified. Two cases are offered to illustrate key points about information sharing across subcultures and some implications for research and practice to enhance abilities within the public sector to appropriately and effectively share information.

Drda-Kȯhn, K. and F. Loseries (2003). Safeguarding performance and quality of cultural work by ICT – Non-technical aspects. e-Society 2003, Lisbon-Portugal, IADIS, International Association for Development of the Information Society.

vertikult is an innovative German research and application project with a three year timeframe at the interface between culture and the arts and the new information and communication technologies. The target is to offer those working in cultural activities an internet-supported platform – an „internet portal" – as an innovative working tool for project work. Via the portal, services can be offered and accepted. Two aspects are new here: this is the first time that such a portal is available in the cultural field covering a complete state and also, further functions will be offered to support the work organisation in projects.

Dufault, M. (2002). The transformation is now: Michigan's innovative formula for e-government success. A Public Sector Case Study. D. Research, Deloitte Consulting: 28.

Dyson, E. (2002). Digital identity management. Release 1.0.

Eaton, J. (1999). "'Open, sesame?' - The problems of digital identity and secure access to information in the Internet era: Issues for the information industry." Business Information Review 16(4): 184-191.

As personal, commercial and legal transactions are increasingly performed electronically, questions of security and proof of identity appear ever more urgent and problematic. The legislative emphasis of national governments has shifted from data protection to defining how 'digital signatures' can be used to certify an individual's identity in electronic transactions. However the old system of password protection is becoming unwieldy, if only because the average employee must now remember 15 different passwords. Reviews the major issues of digital identity and secure access to networked information, analyses the causes of the current discontinuities in access control methodologies and discusses initiatives originating in both the academic and commercial sectors, together with proposed technology driven solutions that depend on Public-Key Infrastructure (PKI). Examines how the electronic information community's primary participants might position themselves in relation to the new era of electronic credentials and argues that successful solutions will be those that acknowledge and enact the characteristics of the contractual relationships between electronic information users, mediators and vendors

Edmiston, K. D. (2003). "State and local e-Government. Prospects and challenges." American Review of Public Administration 33(1): 20-45.

This article presents a self-contained yet comprehensive discussion of the prospects of state and local electronic government (e-government), the status of its development across the states and local communities, and the difficult challenges faced in making it a reality. In taking a very broad approach to e-government, the hope is that the analysis helps to bring perspective to the issue and to synthesize a literature that is increasingly becoming a series of disconnected case studies. Although the prospects at all levels of government for improving public services, reducing costs, and enhancing the democratic process are high, e-government has been penetrating state government much more rapidly than local government. The most salient obstacles to full penetration of e-government seem to be proper marketing, privacy issues, equity, and financing.

Edwards, L. (2003). The problem with privacy: A modest proposal. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

Consumer choice and power is potentially enhanced by the possibilities offered by the Internet, yet simultaneously consumer privacy is threatened. Fears about privacy are well known to be major source of lack of consumer confidence in on line trading, and thus the problem of privacy is one that needs to be addressed if business-to-consumer e commerce is to thrive in Europe. This paper suggests that conventional means of regulating for privacy – via law, norms or "soft law" are both failing to instill consumer confidence and are in any case impossible to enforce in a global cyberspace, both politically and financially. A technological solution, P3P, is being promoted by some US and academic factions but in fact fails to meet the same criticisms as are leveled at law and "soft law". This paper instead sets out an initial framework for

an alternative proposal, in which the common law institution of "trust" is used to attempt to provide the missing element of trust in B2C e commerce.

eEurope (2003). Electronic identity white paper v1.0: 63.

The White Paper presents minimum requirements and other issues that are considered vital when starting to plan and implement e-ID smart card systems based on Public Key Infrastructure (PKI). It was developed by a broad range of interested parties and charters a common way through the complex of international standards and individual national legislative practices. The White Paper is targeted at people and organisations responsible for public e-ID related matters e.g. Certification Authorities (CA), Software vendors, Policy makers, Governments, and other e-ID service providers especially the public officials or other Member State organisations with legal authorization to issue electronic identity cards/certificates for natural persons.

It is structured in three parts:

• minimum requirements for European e-ID-card
• current practices in establishing identity
• e-ID evolution and implementation

The background information on current practices in establishing identity in EU Member States and on the current status of e-ID-card implementations is given to provide the reader with a more complete picture. As the European Union has an advanced regulatory framework for
data protection which determines the implementation of e-ID in the Member States, legal issues in relation to the use of e-ID are also covered to a limited extent. These issues include data protection and the use of biometrics.

Although originating in the eEurope 2002 context the White Paper requirements are equally applicable outside Europe and hence of benefit for others to consult and adopt. By complying with these requirements national authorities responsible for issuing ID can ensure that the ID systems adopted in their own country will interoperate with complying systems in other countries from a technical perspective.

eEurope (2004). Online availability of public services: How is Europe progressing? Web based survey on electronic public services: 55.

This report presents the results of the fourth benchmarking exercise on the progress of online public services in Europe. Next to measuring the percentage of online sophistication of basic public services available on the Internet, this study also measures the percentage of public services fully available online in the 15 EU Member States, plus Iceland, Norway and Switzerland. The survey was executed in October 2003. The European Commission, DG Information Society, ordered the survey in the context of the eEurope programme. The main objective of the benchmark is enabling participating countries to analyse progress in the field of eGovernment and to compare performance within and between countries.

In the following chapter, the context and scope of this study are elaborated. Afterwards, the results of the fourth measurement and the progress that has been achieved compared to the previous measurements are presented. In chapter 4 an analysing framework of the progress is illustrated with good practices. Finally, the overall conclusions on how Europe progressed in the last year are summarised.

Essmayr, W., S. Probst, et al. (2004). "Role-based access controls: status, dissemination, and prospects for generic security mechanisms." Electronic Commerce Research 4(1-2): 127-156.

E-commerce applications have diverse security requirements ranging from business-to-business over business-to-consumer to consumer-to-consumer types of applications. This range of requirements cannot be handled adequately by one single security model although role-based access controls (RBAC) depict a promising fundament for generic high-level security. Furthermore, RBAC is well researched but rather incompletely realized in most of the current backend as well as business layer systems. Security mechanisms have often been added to exist-ing
software causing many of the well-known deficiencies found in most software products. However, with the rise of component-based software development security models can also be made available for reuse. Therefore, we present a general-purpose software framework providing security mechanisms such as authentication, access controls, and auditing for Java software development. The framework is called

GAMMA (Generic Authorization Mechanisms for Multi-Tier Applications) and offers multiple high-level security models (including the aforemen-tioned
RBAC) that may even be used concurrently to cover such diverse security requirements as found within e-commerce environments.

Eyob, E. (2004). "E-government: breaking the frontiers of inefficiencies in the public sector." Electronic Government 1(1): 107-114.

E-government is becoming the preferred tool to enhance seamless government servicesamong its customers and government agencies. It is becoming the next wave of technology applications in the public sector as e-business or e-commerce in the private sector is maturing. This paper uses the 2002 survey of the International City or County Management Association (ICMA) and analyses various issues confronting county and municipality governments in their quest to enable their business processes to become efficient, accurate and ultimately satisfy their clients. However, progress among the survey respondents is mixed. Localities with more resources had more success in e-government implementation, resulting in more government efficiency, as compared to jurisdictions located in rural and large inner cities that lack adeuate funding and the technical wherewithal.

Fassulo, A. and C. Zucchermaglio (2002). "My selves and i: Identity markers in work meeting talk." Journal Of Pragmatics 34(9): 1119-1144.

This paper is concerned with the indexical meaning of the pronoun `I', in its marked use, in Italian work-meeting conversation. The hypothesis driving the study is that, in a context in which situated identities are manifold, marking the pronoun is a device to highlight the most official of one's selves, thus changing the status of the utterance containing the marker. A typology of I-marked utterances is presented and the relative frequency of use is shown to vary with the organizational role of the participants. Detailed analysis of epistemic and performative I-marked utterances shows how role-identities are variously manipulated and mitigated through conversational devices such as self-repair, word delay, and metaphorical work. The discussion highlights how indexical meaning is a property of situated conversational practices and how marked pronouns can foreground selected identities in the cluster of selves that members of a work group can present to each other.

Finger, M. and G. Pecoud (2003). "From e-government to e-governance? Towards a model of e-governance." Electronic Journal of eGovernment 1(1): 1-10.

This paper is conceptual in nature: in it, we seek to identify the current trends of State transformation, combine them with the changes in the new information and communication technologies, and extrapolate this combination into the near future. More precisely, the goal of the paper is to analyse how the New Information and Communication Technologies shape the newly emerging governance mechanisms at local, regional, national, European, and global levels. It furthermore aims at developing a conceptual model in order to understand the evolution towards egovernance, as well as assessing its positive and negative implications for the State and the society at large. Finally, it compares our model with the currently existing definitions and conceptualisations of egovernance and e-government.

Flaherty, D. H. (1979). Privacy and government data banks: An international perspective. London, Mansell.

Flaherty, D. H. (1992). Protecting privacy in surveillance societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill, NC, University of North Carolina Press.

N/A

Fountain, J. E. (2003). Information, institutions and governance: Advancing a basic social science research program for digital government. John F. Kennedy School of Goverment Working Papers Series. Cambridge, MA, Harvard University: 102.

Froomkin, A. M. (1999). "Legal issues in anonymity and pseudonymity." The Information Society 15(2): 113-127.

The regulation of anonymous and pseudonymous communications promises to be one of the most important and contentious Internet-related issues of the next decade. Resolution of this controversy will have direct effects on the freedom of speech, the nature of electronic commerce, and the capabilities of law enforcement. The legal resolution of the anonymity issue also is closely bound up with other difficult and important legal issues: campaign finance laws, economic regulation, freedom of speech on the Internet generally, the protection of intellectual property, and general approaches to privacy and data protection law. The legal constraints on anonymous communication, and the constitutional constraints on those who would regulate it further, thus should be considered in tandem with the policies animating regulation and also their side effects.

Fuchs, G. (2003). Political participation and the Internet. Opportunities and limits of electronic democracy. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

In 2000 for the first time in Germany and may be world wide a virtual party convention was held completely on the Internet. An important result of this experiment was to demonstrate that virtual meetings can be an interesting complementary feature and even a substitute for regular meetings. There are a number of characteristics which are special for virtual meetings which are highlighted in the paper. Advantages and disadvantages will be discussed.

Gamper, J. and N. Augsten (2003). The "eBZ – digital city" initiative. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

Since a few years digital government is becoming an active research area with lots of promises to revolutionise government and its interaction with citizens and businesses. Since up to 80% of transactions between the public administration and its customers take place at the local level, municipalities are the most important access point to government services and information. In this paper we present a new e-government initiative between the Free University of Bozen/Bolzano and the Municipality of Bozen/Bolzano, which aims at fostering the use of information and communication technologies in the local administration. We describe the objectives of the initiative and its context. Two projects have already been started, which are briefly discussed together with first results.

Garson, G. D. (2004). The promise of digital government. Digital government: Principles and best practices. A. Pavlichev and G. D. Garson. Hershey, Idea Group Publishing: 2-15.

E-government promises to mark a new era of greater convenience in citizen access to governmental forms, data, and information. Its advocates promise that not only will egovernment bring the convenience of online transactions, but it will also reverse citizens' disaffection from government, create dramatic savings, and reinforce rather than erode traditional American freedoms and liberties. E-government, however, is better thought of not as a revolution, but as an attempt to bring the e-business model into the public sector. A component-by-component examination of the e-business model shows that it is fraught with problems, challenges, and limitations as well as opportunities. The promise of digital government will be fulfilled only by a new generation of public managers who are generalists, not technocrats, capable of integrating the disparate fields of consideration, which are necessary aspects of the vision of e-government as a whole.

Gasco, M. (2003). "New technologies and institutional change in public administration." Social Science Computer Review 21(1): 6-14.

This article aims to study and analyze, from a multidisciplinary point of view, the organizational and institutional transformations that public administration is experiencing due to a country's transition to the information and knowledge society. Three specific goals are pursued: (a) studying the use of new technologies in the public administration, (b) studying the impact brought about by the use of newtechnologies by the public administration, and (c) studying the institutional changes caused by the use of these technologies. To achieve these goals, three guiding lines are considered: first, the term governance; that is, the collection of institutions and rules that set the limits and the incentives needed for the

constitution and functioning of interdependent networks of actors (government, private sector and civil society actors); second, the new institutionalism perspective; and finally, the relationship between technology and organizational and institutional change.

Gellman, R. (2002). "Perspectives on privacy and terrorism: All is not lost - yet." Government Information Quarterly 19(3): 255-264.

Antiterrorism legislation passed at the end of 2001—the U.S.A. Patriot Act—has serious implications for privacy. Many of the law's provisions expand the government's existing ability to intercept wire, oral, and electronic communications relating to terrorism and other crimes, to share criminal investigative information, and to conduct electronic surveillance. While the changes are controversial, and some are of questionable constitutionality, the surveillance provisions of the new law mostly make changes in degree and not kind. Other aspects of privacy and privacy law remained unchanged. Laws affecting how the private sector gathers, stores, and uses personal information for private purposes were not modified. After passage of the antiterrorism law, other legislation expanded privacy protections in other areas. Further events and legislation will affect privacy rights and interests, and some protections may be eroded while others are improved.

Gengler, B. (2001). "Report: Workplace monitoring tops privacy hit-list." Network Security 2001(2): 5-6.

The technological complexity of workplace surveillance leads the list of top 10 privacy stories of the year 2000, according to a research firm that educates the public on privacy issues.

Germany, T. F. M. o. t. I. o. (2001). eGermany. Joint implementation plan for the federal administration.

Gibson, R. (2002). "Elections online: Assessing Internet voting in light of the Arizona democratic primary." Political Science Quarterly 116(4): 561-583.

Glaessner, T., T. Kellermann, et al. (2004). Electronic security: Risk mitigation in financial transactions. Policy Research Working Paper Series.

This paper builds on a previous series of papers (see Claessens, Glaessner, and Klingebiel, 2001, 2002) that identified electronic security as a key component to the delivery of e-finance benefits. This paper and its technical annexes identify and discuss seven key pillars necessary to the fostering of a secure electronic environment. Hence, it is intended for those
formulating broad policies in the area of electronic security and those working with financial services providers (e.g., executives and management). The detailed annexes of this paper are especially relevant for chief information and security officers responsible for establishing layered security.
First, the paper provides definitions of electronic finance and electronic security and explains why these issues deserve attention. Next, it presents a picture of the burgeoning global electronic security industry. Then, it develops a risk-management framework for understanding the trade-offs and risks inherent in the electronic security infrastructure. It also provides examples of trade-offs that may arise with respect to technological innovation, privacy, quality of service,
and security in the design of an electronic security policy framework. Finally, it outlines issues in
seven interrelated areas that often need attention in the building of an adequate electronic security
infrastructure. These are (i) the legal framework and enforcement; (ii) electronic security of payment systems; (iii) supervision and prevention challenges; (iv) the role of private insurance as an essential monitoring mechanism; (v) certification, standards, and the roles of the public and private sectors; (vi) improving the accuracy of information about electronic security incidents and creating better arrangements for sharing this information; and (vii) improving overall education about these issues as a key to enhancing prevention.

Gray, M. (2003). "Urban surveillance and panopticism: Will we recognize the facial recognition society?" Surveillance & Society 1(3): 314-330.

This paper explores the implementation of facial recognition surveillance mechanisms as a reaction to perceptions of insecurity in urban spaces. Facial recognition systems are part of an attempt to reduce insecurity through knowledge and vision, but, paradoxically, their use may add to insecurity by transforming society in unanticipated directions. Facial recognition promises to bring the disciplinary power of panoptic surveillance envisioned by Bentham - and then examined by Foucault - into the contemporary urban environment. The potential of facial recognition systems – the seamless integration of linked databases of human images and the automated digital recollection of the past – will necessarily alter societal conceptions of privacy as well as the dynamics of individual and group interactions in public space. More strikingly, psychological theory linked to facial recognition technology holds the potential to breach a final frontier of surveillance, enabling attempts to read the minds of those under its g gaze by analyzing the flickers of involuntary microexpressions that cross their faces and betray their emotions.

Gretchen, K. (2002). "Managing the impersonal in a personalized public service." Public Administration and Development 23(2): 197 - 209.

What happens when an apparently personalized small public service enters the information highway? How does it integrate the new frame of mind implied in the impersonal, open approach to information? The practical implications of implementing information technology as a means to use information strategically in the Maltese public service, with its apparently paradoxical administrative style, prompted the pilot study in early 2000 upon which this article is based. Using a simplified empirical approach, the study tested the hypothesis that small scale could affect the way leaders deal with the impersonal, such as information resource management. Although limited in scope, the results of the study support a qualified conclusion that small scale, through its link with personalization and associated informal mechanisms, does affect the way top managers in the public service deal with the impersonal, at least in the short and medium term. To what extent it does so, or the space for change, are subjects for further research. The article concludes with suggestions for further investigation into this topic, both in its narrow and wider applications.

Grewal, D., J. L. Munger, et al. (2003). "The influence of internet-retailing factors on price expectations." Psychology and Marketing 20(6): 477 - 493.

Internet retailing has significantly changed the character of retail competition. More and more often, ordinary consumers, not just the technologically savvy ones, are making purchases over the Internet. The extent to which e-tailers can build trust will significantly influence the willingness of consumers to make purchases over the Internet. As a result, it is important to better understand the factors that influence consumers' trust in e-tailers. This research models the effects of store name, on-line security guarantee, and money-back guarantee on price expectations and willingness to buy. The results suggest that value-enhancing approaches, like assurances of security encryption and money-back guarantees, are more important for less well-known e-tailers than for their more famous competitors.

Groenlund, A. (2003). "Emerging electronic infrastructures. Exploring democratic components." Social Science Computer Review 21(1): 55-72.

The concepts of electronic government and electronic democracy have common roots in that electronic government must rest on, and support, democratic principles. This article discusses how the components of a democratic society are treated as they are built into the emerging electronic infrastructures, dealing with services and dialogues pertinent to the functioning of the public sector, and tries to find emerging patterns. This article opens a discussion on the nature of the emerging infrastructures by reviewing four implementations of local e-democracy and putting them into the context of global e-government development, in particular the European Union’s development of “eEurope.” It is found that the cases represent different models of democracy, models that are only partially explicit. The development is governed more by gradual implementation of information and communication technology than a general political agenda. This means local actors have great influence, and hence, e-democracy is not deterministic; it can come in many shapes.

Gualtieri, R. (1999). Impact of the emerging information society on the policy development process and democratic quality, OECD Public Management Service.

Gunter, C. A. and T. Jim (2000). "Policy-directed certificate retrieval." Software: Practice and Experience 30(15): 1609-1640.

Any large scale security architecture that uses certificates to provide security in a distributed system will need some automated support for moving certificates around in the network. We believe that for efficiency, this automated support should be tied closely to the consumer of the certificates: the policy verifier. As a proof of concept, we have built QCM, a prototype policy language and verifier that can direct a retrieval mechanism to obtain certificates from the network. Like previous verifiers, QCM takes a policy and certificates supplied by a requester and determines whether the policy is satisfied. Unlike previous verifiers, QCM can take further action if the policy is not satisfied: QCM can examine the policy to decide what certificates might help satisfy it and obtain them from remote servers on behalf of the requester. This takes place automatically, without intervention by the requester; there is no additional burden placed on the requester or the policy writer for the retrieval service we provide. We present examples that show how our technique greatly simplifies certificate-based secure applications ranging from key distribution to ratings systems, and that QCM policies are simple to write. We describe our implementation, and illustrate the operation of the prototype.

Gupta, M. P. and D. Jana (2003). "E-government evaluation: A framework and case study." Government Information Quarterly 20(4): 365-387.

The importance of measuring the performance of e-government cannot be overemphasized. In this paper, a flexible framework is suggested to choose an appropriate strategy to measure the tangible and intangible benefits of e-government. An Indian case study of NDMC (New Delhi Municipal Corporation) has been taken up for analysis and placement into the framework. The results obtained suggest that to have a proper evaluation of tangible and intangible benefits of e-government, the projects should be in a mature stage with proper information systems in place. All of the e-government projects in India are still in a nascent stage; hence, proper information flow for calculating 'return on e-government' considering tangible and intangible benefits cannot be fully ascertained.

Halchin, L. E. (2002). "Electronic government in the age of terrorism." Government Information Quarterly 19(3): 243-254.

The events of September 11, and subsequent investigations, suggest that some public information available on the Internet could aid terrorists in planning other attacks. This article provides examples of how federal agency officials have responded to the possibility that their Web sites provide such potentially compromising information. The federal government has not yet issued a government wide policy that addresses this specific contingency. However, the Federal Bureau of Investigation has issued an Internet content advisory and the Attorney General has released a relevant policy statement on the Freedom of Information Act. Both documents are reviewed here. The removal and alteration of information has implications for citizens, as does the Bush Administration's mixed messages on the objectives and procedures of electronic government post-September 11. This article concludes with suggestions for developing a governmentwide Web site-specific policy.

Hansen, M., P. Berlich, et al. (2004). "Privacy-enhancing identity management." Information Security Technical Report 9(1): 35-44.

Privacy-Enhancing Technologies (PET) are the technical answer to social and legal privacy requirements. PET become constituents for tools to manage users' personal data. Users can thereby control their individual digital identity, i.e. their individual partial identities in an online world. Existing commercially available identity management systems (IMS) do not yet provide privacy-enhancing functionality. We discuss general concepts and mechanisms for privacy-enhancing IMS (PE-IMS) in detail and highlight where existing IMS need to be improved in order to deliver them. Derived from general concepts and incorporating existing mechanisms, we define a component-based architecture for PE-IMS. This architecture describes the basic

building blocks a PE-IMS must include, and so it is meant to be used as a fundamental concept for PE-IMS in practice. Finally, we give an outlook on the future development concerning IMS.

Haque, S. M. (2002). "E-governance in India: Its impacts on relations among citizens, politicians and public servants." International Review of Administrative Sciences 68(2): 231–250.

N/A

Harte, A. (2004). "Privacy and identity in a changing world." Australasian Psychiatry 12(1): 56-57.

To consider the issues of privacy and identity relevant to psychiatric practice in the context of recent technological initiatives and the society that has produced them. Conclusions: Emerging technologies may have implications for the ways in which Western society relates. These are likely to affect the ways patients present, their concerns and how we may best assist them. Psychiatry may also be of benefit in the evaluation of the privacy implications of new technologies.

Henriksen, H. Z., D. O. Kerstens, et al. (2004). Public eprocurement in Denmark: Measurements of suppliers' ematurity. 17th Bled eCommerce Conference: eGlobal, Bled, Slovenia.

The paper introduces and evaluates a model for measuring the level of eCommerce maturity for suppliers to the public sector institutions in Denmark. The model comprises four distinct levels and seven parameters. These parameters are related to organizational and technological attributes relevant for eCommerce. Based on an empirical evaluation, it is found that the model is a useful tool for suppliers wanting to evaluate their level of eMaturity. Due to specific requirements from public sector customers it is argued that suppliers to the public sector have to possess a high level of eMaturity.

Herzberg, A. and M. Yosi (2004). "Relying party credentials framework." Electronic Commerce Research 4: 23-29.

We present architecture for a relying-party to manage credentials, and in particular to map different credentials into common format and semantics. This will allow use of simple, widely available credentials as well as more advanced credentials such as public key certificates, attribute certificates and 'negative' credentials (which result in reduced trust) such as certificate revocation lists (CRL). The core of the architecture is a Credential Manager who collects credentials, and maps them to common format and semantics.

Hier, S. P. (2003). "Probing the surveillant assemblage: On the dialectics of surveillance practices as processes of social control." Surveillance & Society 1(3): 399-411.

Recent dialogue on the contemporary nature of information and data gathering techniques has incorporated the notion of assemblages to denote an increasing convergence of once discrete systems of surveillance. The rhizomatic expansion of late modern 'surveillant assemblages' is purported not only to enable important transformations in the p urpose and intention of surveillance practices, but to facilitate a partial democratization of surveillance hierarchies. Seeking to account for the forces and desires which give rise to, and sustain, surveillant assemblages, this paper explicates the workings of a dialectic embedded in many surveillance practices to reveal a polarization effect involving the simultaneous leveling and solidification of hierarchies. Empirical data from the intensification of welfare monitoring are presented to illustrate the dialectics of surveillance practices as processes of social control.

Ho, A. T.-K. (2002). "Reinventing local governments and the e-government initiative." Public Administration Review 62(4): 434-444.

The Internet provides a powerful tool for reinventing local governments. It encourages transformation from the traditional bureaucratic paradigm, which emphasizes standardization, departmentalization, and operational cost-efficiency, to the "e-government" paradigm, which emphasizes coordinated network building, external collaboration, and customer services. Based on a content analysis of city Web sites and a survey of Web development officials, this article shows that many cities are already

moving toward this new paradigm. These cities have adopted "onestop shopping" and customer-oriented principles in Web design, and they emphasize external collaboration and networking in the development process rather than technocracy. The article also analyzes the socioeconomic and organizational factors that are related to cities' progressiveness in Web development and highlights future challenges in reinventing government through Internet technology.

Holliday, I. (2002). "Building e-government in East and Southeast Asia: Regional rhetoric and national (in)action." Public Administration and Development 22(4): 323 - 335.

Among many regional policy initiatives taken by states in East and Southeast Asia in the wake of the 1997 financial crisis, one central project launched by the Association of Southeast Asian Nations (ASEAN), and taken up by its dialogue partners in East Asia, was promotion of information and communication technology. While part of ASEAN's 1999-2004 action plan focused on services for business, another part sought to put public sectors online, and to promote electronic government, or e-government. Taking the 16 states and quasi-states of East and Southeast Asia, this article evaluates progress at the action plan's mid-point in January 2002. It begins by defining e-government and reviewing three academic literatures on the information age, developmental states, and Confucian societies. It then describes the major policy initiatives taken by ASEAN and its partner states, and surveys implementation progress through an analysis of government homepages and sites. Its main finding is that e-government activity in East and Southeast Asia is highly diverse, reflecting national strengths and weaknesses rather than regional capacity for policy change. The article argues for increased attention to national implementation strategies.

Huddy, L. (2001). "From social to political identity: A critical examination of social identity theory." Political Psychology 22(1): 127-156.

Interest in the concept of identity has grown exponentially within both the humanities and social sciences, but the discussion of identity has had less impact than might be expected on the quantitative study of political behavior in general and on political psychology more specifically. One of the approaches that holds the most promise for political psychologists is social identity theory, as reflected in the thinking of Henri Tajfel, John Turner, and colleagues. Although the theory addresses the kinds of problems of interest to political psychologists, it has had limited impact on political psychology because of social identity theorists' disinclination to examine the sources of social identity in a real world complicated by history and culture. In this review, four key issues are examined that hinder the successful application of social identity theory to political phenomena. These key issues are the existence of identity choice, the subjective meaning of identities, gradations in identity strength, and the considerable stability of many social and political identities.

Huemer, L. (2004). "Balancing between stability and variety: Identity and trust trade-offs in networks." Industrial Marketing Management 33: 251– 259.

Both stability and variety are necessary when developing business relationships in networks. This paper identifies a number of trade-offs and traps associated with trust and identity when balancing between stability and variety. It suggests that an organisation’s identity is a stabilising resource, whereas network identification is an activity that may lead to increased variety. Trust is seen as being either passively or actively mobilised. In the former situation, the services rendered from the resource are stabilising due to established procedures and norms. In the latter case, trust is used to gain acceptance for variety by the extended freedom given to other actors.

Humphreys, M. and A. D. Brown (2002). "Narratives of organizational identity and identification: A case study of hegemony and resistance." Organization Studies 23(3).

This paper focuses on issues of identity and identification in a UK-based institution of higher education (Westville (1) Institute). It is suggested that identity, both individual and collective, and the processes of identification which bind people to organizations, are constituted in the personal and shared narratives that people author in their efforts to make sense of their world and read meaning into their lives. The research contribution this paper makes is threefold. First, it illustrates how an organization's identity narrative evolves over time, and the variety of identification narratives, including dis-identification, neutral identification and schizo-identification, in terms of which participants define their relationship to it. Second, it

makes a contribution to what are still rather inchoate efforts to theorize the dynamics of individual--collective processes of identification and identity construction. Finally, it argues that the efforts of senior managers to control processes of organizational identity formation, and participant identification, are interpretable as hegemonic acts required for legitimation purposes.

Hwanga, J.-J., T.-C. Yeh, et al. (2003). "Securing on-line credit card payments without disclosing privacy information." Computer Standards & Interfaces 25: 119–129.

Two revisions of the original Secure Electronic Transaction (SET) protocol are proposed to conceal cardholders' identities in the electronic marketplace in which cardholders' trust for banks can be reduced to a minimum. Constrained by being extensions of the existing card payment networks to the Internet, most on-line credit card payment schemes in use or proposed in recent papers assume the sensitive card information could be disclosed to all the participating banks. The assumption used to work well in traditional credit card payments before. However, negative impacts such as banking scandals, closure programs due to poor management, and security problems with Internet banking are all undermining cardholders' trust in banks. The issuer is the trusted bank selected by the cardholder, but the acquirer is not. To reveal the cardholder's sensitive card information to every possible acquirer implies potential risk. Based on the need-to-know principle, the two revisions are proposed to relax the assumption mentioned above.
In our solutions, the sensitive card information is well protected along the way and can be extracted only by the issuer. A cardholder needs only to select a trustworthy issuer, instead of worrying about the possible breakdowns of every involved acquirer. The cost to achieve our more secure schemes demands only minor information modifications on the legacy system.

IDA (2001). E-government in the service of European citizens and enterprises. What is required at the European level. IDA Sandhamn Conference Conclusions, Sandhamn Hotell & Konferens, Stockholm, Sweden.

IDA (2002). Pan european e government services for citizens & enterprises: The role of IDA, Brussels, Belgium.

The conference was opened by Mr. Erkki Liikanen, European Commissioner for enterprise and information society and Mme. Imelda Read, MEP, and rapporteur for the IDA programme at the European Parliament."If the requirements of cross-border users of e-government services are not taken into account when designing e-government services", said Mr Erkki Liikanen, European Commissioner for enterprise and information society, opening the conference, "these may even create unintentional barriers to the continued development of the single market. For enterprises, this could mean a relative loss of competitiveness and increased costs for citizens".Mme Imelda Read, MEP, and rapporteur for the IDA programme at the European Parliament, noted that: "It is probable that e-government services will play a key role in re-engaging the public with political institutions and public organisations. As an MEP I am regularly approached by constituents who need help to liase with public bodies in other Member States. Well developed e-government services could be very effective in this field".Separate parallel sessions were devoted to the needs of both citizens and enterprises for pan-European e-government services, and to the provision of such services in the Member States. The conclusions of the parallel sessions were presented to the conference in plenary sessions. Based on the inputs from the parallel sessions, the conference, meeting in plenary, discussed the development of a strategy for pan-European e-government services, which was subsequently, presented to the closing session, chaired by Mr Jean-Paul Mingasson, Director General for the Enterprise Directorate General (European Commission).This report analyses the conclusions derived by each working group, brings out areas of commonality and summarises the conclusions under common topic headings. The envisaged audience of this report is all those concerned with the delivery of e-government services in Europe. These include public management and e-government Ministers, public management and e-government Directors General, the European Commission and its services as well as the other European institutions, the members of the IDA TAC (Telematics between Administrations Committee), and the participants at the Brussels conference.

IDA (2002). Survey on egovernment services to enterprises.

IDA (2003). Linking-up Europe: The new IDA publication. Commission Staff Working Paper. E. D.-G. The Commission of the European Communities. European Communities, IDA: 23.

The purpose of the working paper is to obtain acceptance from key decision and policy makers in Europe on the need for interoperability both within and between administrations and with the enterprise sector. It seeks to obtain the necessary commitments for this to happen at all levels (i.e. European, national, regional and local) and to ensure that any consequential adjustments of European or national policies occur. As Europe's citizens move between Member States and enterprises trade across Europe's borders they need to transact business Europe's public administrations. Increasingly these transactions will be carried out electronically. They may well need to interact with public administration IT systems in other Member States the same way as national public administration bodies must co-operate in the provision of e-government services at the national level. The working paper deals with these issues, and focuses on what is required to ensure that the back-office system of Europe's public administrations are sufficiently interoperable to allow seamless pan-European e-government services to be developed.

Institute, D. T. (2004). Reorganisation of government back-offices for better electronic public services – European good practices
(back-office reorganisation) Annex 6.

Institute, D. T. (2004). Reorganisation of government back-offices for
better electronic public services – European good practices (back-office reorganisation)
Annexes 1 to 5. 2.

Jaeger, P. T. (2003). "The endless wire: E-government as global phenomenon." Government Information Quarterly 20(4): 323-331.

Jaeger, P. T. and K. M. Thompson (2003). "E-government around the world: Lessons, challenges, and future directions." Government Information Quarterly 20(4): 323-331.

Jaeger, P. T. and K. M. Thompson (2004). "Social information behavior and the democratic process: Information poverty, normative behavior, and electronic government in the United States." Library & Information Science Research 26(1): 94-107.

Electronic government (e-government) is the provision of government information and services through the Internet to citizens and businesses and among government agencies. This electronic manifestation of government offers new levels of access to government information and services. However, if e-government usage is limited in certain segments of society, it is not achieving its egalitarian potential. Understanding reasons why people do not use e-government will facilitate the development of a more inclusive e-government that better fulfills its potential to deliver information to all citizens and increase participation in the democratic process. Two phenomena of information behavior, information poverty and normative behavior, may help explain why certain groups do not use e-government information. This article offers suggestions on how these concepts of information behavior can contribute to the e-government research agenda.

Jefries, F. I. and R. Reed (2000). "Trust and adaptation in relational contracting." Academy of Management Review 25(4): 873-882.

Trust, which occurs at the organizational and interpersonal levels, is generally believed to be important for the success of interfirm relationships. The authors explore the effects of interaction between the two types of trust on negotiators' motivation to solve problems of adaptation in relational contracting. Findings suggest that too much trust is as bad as too little. Solutions are furthest from optimal when both organizational and interpersonal trust are high or both are low.

Jenlink, P. M. and B. H. Banathy (2002). "The agora project: The new agoras of the twenty-first century." Systems Research and Behavioral Science 19(5): 469 - 483.

The Agoras of the City States of the Classical Greeks were public spheres where democracy was lived by citizens who made collective decisions about issues affecting their daily lives. The Agora Project - New Agoras - is a metaphor for social action contexts in which people can make collective decisions about their future. People in the settings of their families, neighborhoods, community groups, organizations and institutions have the potential to organize themselves as evolutionary design communities. Participants in the Agora Project collectively enjoin to establish a new public sphere that can sustain a meaningful actionable design dialogue among individuals within and across New Agoras. These New Agoras, communicatively linked, would serve as the infrastructure for democratic civil society and a system of public spheres animated by evolutionary conversation and guided by evolutionary design with purpose of self-guided evolution of the society - cultural evolution of our species, Homo sapiens sapiens. Critical to the Agora Project is the establishment of stewardship communities. The task of these communities is to create knowledge bases for evolutionary inquiry, develop resources for evolutionary learning and explore suitable approaches, methods and technologies. This article will present an overview of the Agora Project and the Agora Steward Community that has evolved in relation to the project. Organization of the article includes: (1) an examination of the evolution of humankind, (2) a discussion of conscious purposeful evolution, (3) an examination of the Agora of ancient Athens, (4) an introduction of the New Agoras as a metaphor for social action in contemporary society, (5) a discussion of the New Agoras as public spheres for democratic civil society, (6) a description of the Agora Project, and (7) a discussion of the New Agoras as public spheres for evolutionary design.

Joaquim, R., A. Zïquete, et al. (2003). REVS – A robust electronic voting system. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

There are many protocols proposed for electronic voting, but only a few of them have prototypes implemented. Usually the prototypes are focused in the characteristics of the protocol and do not handle properly some real world issues, such as fault tolerance. This paper presents REVS, a robust electronic voting system designed for distributed and faulty environments, namely the Internet. The goal of REVS is to be an electronic voting system that accomplishes the desired characteristics of traditional voting systems, such as accuracy, democracy, privacy and verifiability. In addition, REVS deals with failures in real world scenarios, such as machine or communication failures, witch can lead to protocol interruptions. REVS robustness has consequences at three levels: (i) the voting process can be interrupted and recovered without weakening the voting protocol; (ii) it allows a certain degree of failures, with server replication; and (iii) none of the servers conducting the election, by its own or to a certain level of collusion, can corrupt the election outcome.

Joia, L. A. (2004). Government-to-government enterprises in Brazil: Key success factors drawn from two case studies. 17th Bled eCommerce Conference: eGlobal, Bled, Slovenia.

Recently, various governments have seized the moment provided by Information and Communication Technology as the ideal opportunity to rethink and reformulate their administrative praxis. The digitally-enabled collaboration and cooperation perspective among different government agencies - commonly referred to by the acronym G2G (Government to Government) - is the main focus of this study. Consequently, this work seeks to analyze the key factors for successful implementation of G2G projects. In order to achieve this, multiple case study explanatory methodology based on two recent reallife cases was adopted. From these case studies, the critical success factors in the implementation of Government-to-Government processes between public agencies in Brazil are studied. Finally, some conclusions are drawn and further research is presented in order to assist policy makers and public administrators in dealing with this new field of knowledge adequately.

Jones, G. R. and J. M. George (1998). "The experience and evolution of trust: Implications for cooperation and teamwork." Academy of Management Review 23(3): 531-546.

In this article we analyze the way that trust evolves in organizations and how it influences cooperation and teamwork. We propose that the experience of trust is determined by the interplay of

people's values, attitudes, and moods and emotions. Then, using the perspective of symbolic interactionism, we examine how trust evolves and changes over time, describing two distinct states or forms of trust: conditional and unconditional. We look, too, at the factors involved in the dissolution of trust. Finally, we explore the relationship between trust and an important component of organizational performance and competitive advantage: interpersonal cooperation and teamwork.

Jones, S., M. Wilikens, et al. (2000). "A conceptual framework for understanding the needs and concerns of different stakeholders. Trust requirements in e-business." Communications of the ACM 43(12): 80-87.

Jones, S. G., Ed. (1997). Virtual culture: Identity and communication in cybersociety. London, Sage.

Kampen, J. K. and K. Snijkers (2003). "E-democracy. A critical evaluation of the ultimate e-dream." Social Science Computer Review 21(4): 491-496.

In this article, the authors examine the possibilities of information communication technology and e-government to enhance democracy. The authors summarize the known problems of representative democracy and direct democracy and inquire whether e-government potentially can offer solutions to these problems. The authors conclude that a lot of problems in both representative and direct democracies remain unsolved and that e-government even can create new problems.

Kantner, C. (2005). What is a European identity? The emergence of a shared ethical self-understanding in the European Union. EUI Working Papers. Florence, European University Institute, Robert Schuman Center for Advanced Studies.

Against the common view that a European identity is a functional precondition for legitimate EU governance, this paper argues that conceptual weaknesses of the term 'collective identity' inherited from social philosophical and sociological tradition led to a confusion of several analytic dimensions of 'identity' and to an overestimation of strong forms of collective identity. Insights provided by analytic philosophy will be introduced in order to redefine and differentiate the concept of 'collective identity'. The ways in which people refer to themselves as members of we-groups will be outlined in order to contribute to an innovative model of the problem and therefore policy-related formation of collective identities. In each sub-section the relevance of these conceptual considerations for evaluating whether or not 'the Europeans' see themselves as members of a community will be shortly illustrated. The paper concludes that a strong European identity is not a functional precondition for legitimate democratic governance in the EU as far as every day politics is concerned. Only in extraordinary situations and in order to institutionalise integration in ethically sensitive policy fields is it necessary that the EU-citizens discursively agree on an ethical self-understanding of their way of life.

Karmakar, N. L. (2003). Digital security, privacy & law in cyberspace: A global overview. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

Every day the news media give us more and more insight into the effects of digital security on our daily lives. Due to the enormous power of computer & communication technologies (ICTs), any lack of digital security affects privacy and ethics. The commercialisation of the Internet has stimulated considerable competition, both legitimate and illegitimate. The law governing intellectual property is not adequate to control the huge amount of information contained in cyberspace, which is defined as the realm of digital transmission not limited by geography. The change in the legal system is evolutionary, but the technological change is revolutionary. The immediate need for organizations to protect critical information assets continues to increase. It is a difficult task to establish a common international legal framework to maintain security and privacy in cyberspace. The new business environment, due to the explosion of Electronic Commerce (EC), has new security, privacy, legal and ethical problems that business people in the digital economy must be acquainted with, in order to handle them properly, and operate them effectively. The objective of this paper is to provide a global overview of major concerns in cyberspace as stated above. The author also discusses the Australian response to deal with those key concerns in the era of digital economy and globalisation.

Kenny, S. "Managing EU implications: EU data protection for transitional societies." Convergence 4(1): 20-23.

Data management must be compliant with EU data protection law if the data is collected in the EU, but processed in transitional societies. A privacy specialist with combined technical and legal expertise drives the development, interpretation and implementation of this framework.

Kenny, S. and L. Korba (2002). "Applying digital rights management systems to privacy rights management." Computers & Security 21(7): 648-664.

While there are growing concerns about how to manage citizen privacy, currently there are no established technology solutions that meet the privacy needs required in some cases by legislation. In this paper we examine the prospect of adapting systems developed for Digital Rights Management to meet the challenges of Privacy Rights Management. In particular, the goal of this work is the adaptation of DRM technology to produce a privacy management architecture that reflects the requirements of Directive 95/46/EC for the protection of personal data. This paper first outlines the requirements for management of the personal data within the European Community it then describes the changes that would be required to transform a digital rights management system into a system to manage the handling of personal data. The paper concludes with a thorough discussion of the issues and potential of this approach.

Kessler, T. and A. Mummendey (2002). "Sequential or parallel processes? A longitudinal field study concerning determinants of identity-management strategies." Journal of Personality and Social Psychology 82(1): 75-88.

Using a longitudinal field design, this study tested the dynamics of an integrative model of social identity theory (SIT) and relative deprivation theory (RDT) with regard to relations between perceived sociostructural characteristics, perceived in-group identification, perceived fraternal deprivation (i.e., resentment) and identity-management–strategy preference. Trait–state analyses revealed that the dynamic relationship among constructs in the model can best be explained in terms of trait-dependent variation rather than sequentially ordered processing. The trait components of the variables replicate previous findings concerning SIT and RDT. However, stable functional relations between variables and their traitlike character contradict the notion that their underlying processes are linear and sequential. Rather, variables and their relations can be regarded as the product of parallel processes. The authors discuss the results as a challenge to core assumptions of SIT.

King, R. B. (2003). "Security maintenance mediation: A technology for preventing unintended security breaches." Concurrency and Computation: Practice and Experience 16(1): 49 - 60.

Web-resident information is becoming smarter, in the sense that emerging technology will support the annotation of it with ontological terms, which will be used to locate and reuse information. This will pose a great security risk in the form of unintended breaches (as distinct from deliberate invasions). Web-resident information will be far more readily available and relevant, thus causing inadvertent releases of secure information to potentially cause it to be diffusely spread across the Internet. Then as this information is iteratively transformed and integrated with other information, it will become irretrievable and potentially used in a myriad of unpredictable ways. The problem is that ontological annotations, while making information more understandable in its original form, do not provide a means for easily capturing the complex semantics of information that has been transformed via abstraction, aggregation, and integration. This demands the development of a semantically rich way of specifying views of Web information, to which security controls can be attached. Also needed is a way for users of secure information to easily and voluntarily blend - and thereby propagate - security controls as information is transformed. Information mediators designed by collaborative teams of experts are proposed as the vehicle for wrapping information, so that at each step of reuse, high-level views and their corresponding integrity controls can be made easily accessible to trusted users who will then be able to ensure their proper maintenance.

Kitcat, J. (2004). "Government and ICT standards: An electronic voting case study." Info, Comm & Ethics in Society 2(3): 143-158.

This paper examines and illustrates the process of settind technical intercommunication standards through a case-study taken from the electronic voting industry. It begins by addressing the large number of types of standards and the many ways in which they are created. The tensions between the speed to market, stakeholder invalvement, the mode of production and the legitimacy of a standard are explored. The modes of standards production are then presented in a linear model. The preceding discussion sets the context for a case which presents attemps to standardise the large number of of competing electronic voting solutions. The importance of which actors back and influence a standard's development up to successful adoption is exposed. The vital role government can play in preventing a standards market failure is raised and recommendations are offered on how governments can improve their contributions to standardisation.

Kleist, V. F. (2004). "A transaction cost model of electronic trust: Tansactional return, incentives for network ecurity and optimal risk in the digital economy." Electronic Commerce Research 4: 41-57.

Transaction cost economics can explain the mechanism by which network security technologies may reduce the interexchange costs between businesses in the supply chain and between businesses and customers in the digital economy. This paper develops the construct of technology-based electronic trust, where interpersonal, or "real" trust between people can be amplified and enhanced with the use of network security information technologies.

The paper formally models an electronic commerce trust typology based on minimizing the cost of establishing trust in transactions, balanced against maximizing the potential user value from successfully completing transactions in the digital economy, suggesting that there is an optimal amount of acceptable risk in electronic commerce transactions. Sophisticated deployments of security information technologies may increase levels of interper-sonal

trust while lowering transaction costs in electronic commerce, thus promoting the long run development of neutral, interorganizational electronic markets and growth in the digital economy.

Knights, D. and H. Willmott (1999). Management lives! Power and identity in work organizations, SAGE.

Koch, M. and W. Worndl (2001). Community support and identity management. ECSCW 2001, Bonn, Germany.

Computer based community support systems can provide powerful support in direct exchange of information and in finding people for information exchange. Such applications usually make use of information about the user (user profile information) for personalization and for supporting contact management. As in real life, a user will interact with different communities (community support applications) hosted by different providers. With the current approach users have to provide and update information about their identity and interests for each community independently. That results in cold-start problems with new community support applications and in inconvenience for the user. In this

paper we discuss user-centric identity management for community support applications and concentrate on a platform for using user profiles in more than one application. We also propose mechanisms to address privacy issues in this framework.

Kongas, O. (2002). eFinland. Aim of public management: Further development of electronic transactions, Finnish Ministry of Finance.

Korba, L. and S. Kenny (2002). Towards meeting the privacy challenge: Adapting DRM.

There are many requirements for achieving the privacy needs as expressed in law. Currently there is no commonly accepted technical approach for meeting these privacy requirements. An often-fruitful way for uncovering solutions to new challenges is to examine how current technologies used in quite different applications may be adopted to meet the specific challenges. In this paper, we examine the prospect of adapting systems designed for Digital Rights Management for the purpose of Privacy Rights Management for European Community application. We begin by outlining the legal requirements for privacy under the

European Union Data Directive. After an overview of digital rights management systems, we describe adaptations for transforming a DRM system into a privacy rights management system. In the conclusions we detail the strengths and weaknesses of the approach.

Koskela, H. (2003). ""Camera" – the contemporary urban panopticon." Surveillance & Society 1(3): 292-313.

Deriving from Foucault's work, space is understood to be crucial in explaining social power relations. However, not only is space crucial to the exercise of power but power also creates a particular kind of space. Through surveillance cameras the panoptic technology of power is electronically extended. The article examines parallelisms and differences with the Panopticon and contemporary cities: visibility, unverifiability, contextual control, absence of force and internalisation of control. Surveillance is examined as an emotional event, which is often ambivalent or mutable, without sound dynamic of security and insecurity nor power and resistance. Control seems to become dispersed and the ethos of mechanistic discipline replaced by flexible power structures. Surveillance becomes more subtle and intense, fusing material urban space and cyberspace. This makes it impossible to understand the present forms of control via analysing physical space. Rather, space is to be understood as fundamentally social, mutable, fluid and unmappable – 'like a sparkling water'. The meaning of documentary accumulation changes with the 'digital turn' which enables social sorting. The popularity of 'webcams' demonstrate that there is also fascination in being seen. The amount of the visual representations expands as they are been circulated globally. Simultaneously the individuals increasingly 'disappear' in the 'televisualisation' of their lives. The individual urban experience melts to the collective imagination of the urban. It is argued that CCTV is a
bias: surveillance systems are presented as 'closed' but, eventually, are quite the opposite. We are facing 'the cam era' – an era of endless representations.

Kostopoulos, G. K. (2003). E-government in the Arabian gulf: A vision toward reality. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

This paper presents a review of the e-government initiatives in the Arabian Gulf countries that form the Gulf Cooperation Council, GCC. Throughout the region, extensive efforts are being made to capitalize on the cyber technologies and enhance the government to citizen service. The described cases are from Kuwait, Bahrain, Saudi Arabia, Qatar, the United Arab Emirates and Oman. While the efforts vary in size and intensity, what appears to be common is the top level support the e-government initiatives are receiving, which offers them visibility and hopefully warrants their eventual success. The collective message delivered by the examined cases is that e-government is becoming an integral part of the respective countries life with a byproduct being an increase in society's cyber-literacy.

Kurth, J. (2003). "Reinventing Identities in the Atlantic World: British identity between three empires." Orbis 48(1): 161-171.

La Porte, T. M., C. C. Demchak, et al. (2002). "Democracy and bureaucracy in the age of the web. Empirical findings and theoretical speculations." Administration & Society 34(4): 411-446.

The foundations for governance in an information age are developing through the World Wide Web as it becomes the principal electronic public gateway into government organizations. Governmental openness is now important to a variety of strategies for governmental reform. The Web (a) makes government more efficient; (b) facilitates the functioning of new networklike arrangements between public organizations, the private sector, and citizens; and (c) empowers citizens to play a stronger role in interacting with government.We describe the concept of organizational openness and summarize a methodology to measure it on a worldwide basis. Data from 1997 through 2000 are presented, showing rapid diffusion of the Web and variation in levels of openness, even across countries with similar levels of economic and political development. Bureaucracies adopt Web technologies as a function not of traditional diffusion processes, but of emergent institutional isomorphism. Short-term prospects for responsive government improve, but so do unrealistic expectations affecting government legitimacy.

Lamm, G. A. and Y. Y. Haimes (2002). "Assessing and managing risks to information assurance: A methodological approach." Systems Engineering 5(4): 286 - 314.

Recent events such as the September 11th attack, the Yahoo! denial-of-service attack, the I Love You virus, and the Code Red worm have sparked a dramatic interest in assuring the future security of information infrastructures. Information systems are increasingly interconnected, interdependent, and complex. Information assurance (IA) attempts to answer critical questions of trust and credibility associated with our digital environment. It presents myriad considerations and decisions that transcend many dimensions: technological advancement, legal, political, economic, social, cultural, institutional, organizational, and educational. Despite the millions of dollars spent on firewalls, encryption technologies, and intrusion detection software, information infrastructure vulnerabilities and disruptive incidents continue. These trends have a significant impact on military operations now and for the next decades. This paper identifies and develops a methodological framework for assessing and managing IA risks. The methodology is based on the systems engineering design process as well as on the guiding principles of risk assessment and management. It builds on hierarchical holographic modeling (HHM) and risk filtering, ranking, and management (RFRM). HHM identifies a plethora of risk scenarios and sources of risk that are innate in current complex information systems. The flexibility of the HHM philosophy permits limitless representations of systems perspectives, constrained only by the knowledge, creativity, and imagination of the analyst and the appropriateness of the modeling efforts. RFRM is an eight-phase process that filters the hundreds of risk scenarios down to a manageable few (10-20), and ranks them. The risk management phase then identifies the acceptable policy options and analyzes the tradeoffs among them by using quantifiable risk management tools. This process analyzes the wealth of statistical data on losses due to system failures, to intrusions, or to vulnerabilities of information assurance.

Lampard, L. (1997). "Government departments: Developments in the delivery of information." Business Information Review 14(4): 179 -183.

The rapid increase in UK government information, brought about by restructuring, Next Steps programme, Citizen's Charter and Open Government, makes it increasingly difficult for users to trace and exploit what is available. Examines the influence of these factors on the growing numbers of CD-ROM and online databases and faxback services with particular reference to the adoption of the Information Society Initiative strategy which aims to make every UK individual able and confident in using the latest information technology. Pays particular attention to the availability of information sources from the government and government departments via the Internet and World Wide Web noting: the availability of Hansard on the Internet; the Access Business project; and the setting up by the Cabinet Office of the direct.link service for organizations providing public services electronically. Concludes with brief notes on other non-Internet electronic sources of government-related information.

Larson, G. S. and G. L. Pepper (2003). "Strategies for managing multiple organisational identifications." Management Communication Quarterly 16(4): 528-557.

This case study reveals how organization members communicatively manage multiple targets and sources of identification during a time of company transition.Interview accounts are used to examine how members discursively construct understanding as they discuss two competing value-based identity structures.Results reveal three distinct discursive strategies —comparison, logic, and support —that members use to manage identity tensions,and eight corresponding communicative tactics used to enact those strategies.This focus on communicative strategies and tactics is important because identities are expressed through language,and discourse is the means available to organization members for negotiating various identity structures. Discursive strategies are central to the identity formation process and provide a window into the sensemaking of participants.

Laur, U. and K. Koit (2003). Electronic access to legal acts in Estonia, Department of Information Systems and Document Management at the Estonian State Chancellery.

Legal, M., S. Papadopoulou, et al. (2002). Cross-border business intermediation through electronic seamless services.

As it is pointed out in a recent consultation document produced by the European Commission [European Commission 2002], implementations of e-Government services are not open to cross-border users and generally e-Government services are designed without having in mind the encouragement of trans-European mobility and cross-border e-business. On the other hand,as testified by the results of a survey carried out by the e-Government Observatory [e-Government Observatory 2002], enterprises assign high importance to the availability of cross-border
administrative services and appreciate facilitated access to e-services of all Member States.The CB-BUSINESS project, aiming to develop an intermediation platform that will facilitate cross-border interactions between public authorities and enterprises, contributes to filling up the existing gap and meeting the business needs for interacting and transacting in cross-border settings. The objective of this deliverable is to present the results of a relevant state-of-the-art analysis.This analysis has been designed so as to investigate, on the one hand, ongoing initiatives and projects in the area of electronic government that address the issue of cross-border interactions, and review, on the other hand, the state-of-the-art in technical and methodological fields related to the CB-BUSINESS project.The scope of review reflects this mixed balance of interests by including non-technological themes that apply to our overall operational approach,such as one-stop e-Government service schemes (section 2), on-going projects and initiatives for cross-border business processes (section 4) and performance measurement and management methodologies for the public sector (section 5), as well as technological themes that apply to our proposed technical solution, such as workflow management systems, portal development platforms and web services (sections 3.1, 3.2, 3.3 respectively).

Leitner, C. (2003). eGovernment in Europe:The state of affairs. eGovernment 2003 Conference, Como, Italy.

Lianos, M. (2003). "Social control after Foucault." Surveillance & Society 1(3): 412-430.

After the Foucauldian model, often misunderstood and projected without nuance onto the present, the study of social control has not progressed much. Meanwhile, changes on the ground call for the construction of a new theoretical paradigm which should take account of three contemporary tendencies: a) the embedding of control in the widespread and often consensual interaction between the user and the outlets and systems of institutional action; b) the emergence of an 'unintended control', that is not oriented towards values; and, c) the inherent contribution of sociotechnical systems, which at once regularise social behaviour and project onto their users a consciousness formed around invisible, yet ubiquitous, threats. The paper proposes to understand these tendencies as part of the contemporary transition towards institutional normativity and institutional sociality, two concepts that the author has developed in other works.

Liberatore, A. (2005). Balancing security and democracy: The politics of biometric identification in the European Union. EUI Working Papers. Florence, European University Institute, Robert Schuman Center for Advanced Studies.

What are the relations between security policies and democratic debate, oversight and rights? And what is the role of expertise in shaping such policies and informing the democratic process? The inquiry that follows tries to answer such questions in the context of the European Union and taking the case of biometric identification, an area where security considerations and the possible impacts on fundamental rights and rule of law are at stake, and where expertise is crucial. Some hypotheses are explored through the case study: that 'securitisation' and 'democratisation' are in tension but some hybrid strategies can emerge, that the plurality of 'authoritative actors' influences policy frames and outcomes, and that knowledge is a key asset in defining these authoritative actors. A counter-intuitive conclusion is presented, namely that biometrics-which seems prima facie an excellent candidate for technocratic decision making, sheltered from democratic debate and accountability-is characterised by intense debate by a plurality of actors. Such pluralism is limited to those actors who have the resources-including knowledge-that allow for inclusion in policy making at EU level, but is nevertheless significant in shaping policy. Tragic events were pivotal in pushing for action on grounds of security, but the chosen instruments were in store and specific actors were capable of proposing them as a solution to security problems; in particular, the strong role of executives is a key factor in the vigorous pursuit of biometric identification. However this is not the whole story, and limited pluralism-including plurality of expertise-explains specific features of the development of biometrics in the EU, namely the central role of the metaphor of 'balancing' security and democracy, and the 'competitive cooperation'

between new and more consolidated policy areas. The EU is facing another difficult challenge in the attempt of establishing itself as a new security actor and as a supranational democratic polity: important choices are involved to assure that citizens' security is pursued on the basis of rule of law, respect of fundamental rights and democratic accountability.

Lyon, D. (2001). Surveillance society: Monitoring everyday life. London, Open University Press.

Lyon, D. (2002). "Everyday surveillance: Personal data and social classifications." Information, Communication and Society 5(2): 242 -257.

Surveillance is no longer merely a matter of deliberate, individual scrutiny and consequent fears for personal privacy. It is an everyday experience, run by myriad agencies for multiple purposes and exempting no one. Surveillance is also an ambiguous process, the two faces of which must yet be seen in relation to each other. Numerous data - now including biometric, genetic and video data - are abstracted from embodied persons and manipulated to create profiles and risk categories in a networked, rhizomic system. The resulting classifications are intended to influence and to manage populations and persons. The choices and the chances of data-subjects are thus both directly and indirectly affected, but socio-technical surveillance systems are also affected by people complying with, negotiating or resisting surveillance

Macintosh, A., E. Robson, et al. (2003). "Electronic democracy and young people." Social Science Computer Review 21(1): 43-54.

This article examines action to address young people's apathy to the democratic process and politics in general, by considering possibilities for using information and communication technology to engage young people. The article describes two e-democracy systems in use in Scotland, which provide young people with opportunities to participate in and understand democratic decision making. The systems are designed to allow young people to deliberate issues of importance to them. The Highland Council initiative involves young people in the design of a web site for their youth parliament with online debates and Internet voting. The Young Scot initiative is a national youth portal, including an e-democracy channel. The emphasis here is on content management and moderation of e-consultations for young people. Research indicates that democracy is best taught by practicing it and that many young people are comfortable using new information and communication technologies. These ideas
form the basis of both projects.

Mack, A., Ed. (2001). Privacy - Proceedings of the conference at New School University, Social Research.

Madsen, W. (2001). "FBI documents show scope of internet surveillance." Computer Fraud & Security 2001(1): 5-6.

According to documents released to the Electronic Privacy Information Center (EPIC) on 4 December 2000, the Federal Bureau of Investigation (FBI) is not only expanding the role of Carnivore to interact with other electronic surveillance systems but is marketing the tool to other Federal and state law enforcement agencies. The documents were released pursuant to a Freedom of Information Act request and a subsequent US Federal Court order.

Mahler, J. and P. M. Regan (2002). "Learning to govern online. Federal agency Internet use." American Review of Public Administration 32(3): 326-349.

This research offers a limited empirical study of online service in federal government agencies. The authors are interested in the evolution of online governance and what factors influence the adoption and elaboration of online services. Information about online agency services was gathered primarily from online U.S. General Accounting Office reports and testimony offered between 1993 and 2000. The authors examine online activities that carry out three governmental functions: providing services, collecting information, and

soliciting stakeholder comment. Four principal cases were selected: the Social Security Administration's Online PEBES, the Department of Education's National Student Loan Data
System, the Securities and Exchange Commission, and the Nuclear Regulatory Commission. The analysis of these cases identifies a partial sequence of steps or stages in development of online services. It appears that this sequence is a result of both learning and the imposition of certain standards of performance based on best practices and legislative mandates.

Mann, S., J. Nolan, et al. (2003). "Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments." Surveillance & Society 1(3): 331-355.

This paper describes using wearable computing devices to perform "sousveillance" (inverse surveillance) as a counter to organizational surveillance. A variety of wearable computing devices generated different kinds of responses, and allowed for the collection of data in different situations. Visible sousveillance often evoked counter-performances by front-line surveillance workers. The juxtaposition of sousveillance with surveillance generates new kinds of information in a social surveillance situation.

Martin, B. and J. Byrne (2003). "Implementing e-government: Widening the lens." Electronic Journal of eGovernment 1(1): 11-22.

In this paper progress towards e-government is perceived as contributing to the ultimate development of a Europe-wide Information Society. We consider aspects of the development EU countries have made towards Information Society status. In the process we review current criteria and demonstrate their strong technoeconomic characteristics. We suggest that broader perspectives should be adopted in implementing egovernment. We identify some potential societal criteria necessary to attain the vision of an Information Society.

Martin, D., M. Rouncefield, et al. (2002). Applying patterns of cooperative interaction to work (re)design: E-government and planning. Conference on Human Factors in Computing Systems. Proceedings of the SIGCHI conference on Human factors in computing systems: Changing our world, changing ourselves, Minneapolis, Minnesota, USA.

This paper presents patterns of cooperative interaction derived from ethnographic studies of cooperative work as devices for generalisation, re-use and design. These patterns consist of examples of similar social and interactional phenomena found in different studies that serve as resources for defining and envisaging design concepts, and potential work process and technical solutions. We outline new pattern examples and demonstrate their use in application to a complex setting: e-government in local government planning

Mavridis, I. K. Georgiadis, et al. (2002). "Access-rule certificates for secure distributed healthcare applications over the Internet." Health Informatics Journal 8(3): 127-137.

Access control in medical information systems distributed over the Internet is an important issue directly related to the protection of patients' privacy. It is therefore essential to satisfy the increasing demand for exploiting Internet mechanisms in order to achieve a secure health information network. This can only be done, however, if it can be guaranteed that appropriate measures have been taken to preserve a satisfactory level of security for the information concerned. Recent efforts in this direction rely on public-key cryptography and digital certificates. Identity certificates are suitable for identification and authentication purposes. In addition, attribute certificates are another type of certificate particularly suitable for authorization purposes. In order to fully exploit digital certificates to protect distributed healthcare applications over the Internet, we propose the use of a third type of certificate, called access-rule certificates, which are useful for the enforcement of global access-control mechanisms between different organizations. In this paper, we present the structure of those three types of certificate, as well as the access-control procedures when using them; we describe the architecture of the proposed system whose purpose is to explore the use of certificates for the implementation of a suitable security policy for healthcare environments.

Mayer, R. N. (2003). "Technology, families, and privacy: Can we know too much about our loved ones?" Journal of Consumer Policy 26(4): 419- 439.

Both an array of privacy advocates and a body of privacy policies have emerged to reduce threats to personal privacy posed by Big Government and Big Business. Technologies that threaten personal privacy when employed by large institutions are increasingly being used by family members to track one another, but without a comparable level of societal scrutiny and control. This paper examines four such technologies - Internet tracking software, global positioning systems, miniature cameras, and genetic tests - to gauge their level of use and public acceptance and then to consider their impact on family relations, especially those between parent and child and between spouses. While these technologies are intended to promote the safety of family members, by disrupting personal privacy, they may also provoke a number of counterproductive responses that reduce safety. Moreover, the deployment of these technologies may inhibit the development of trust and trustworthiness within the family. Partly owing to a lack of understanding of how new technologies affect family relations, both formal and informal efforts to control these technologies have been slow to develop.

McPherson, M. and S. Field (2003). Are UK local authorities on the right path to egovernment? e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

ICT is pervading every sphere of life in the 21st Century, and government circles are no exception. In 2000, the UK government presented its vision of citizens and organisations being able to access local and national government services through electronic communications and set ambitious target for all Government services to be on-line by the year 2005. Research was undertaken at the University of Sheffield to assess some of the approaches adopted by a selection of Local Authorities to meet these targets. The study concentrated on efforts of Local Authority "Pathfinders", who were chosen as pioneers of eGovernment implementation. Particular attention was paid to the issue of how local authorities intended to minimise the social exclusion through the digital divide.

Meier-Pesti, K. and E. Kirchler (2003). "Attitudes towards the Euro by national identity and relative national status." Journal of Economic Psychology 24: 293 –299.

The present study investigates the effect that the relative status of a nation in the European Monetary Union –in this case Austria –and national identity has on attitudes towards the Euro. Alternative assumptions deriving from social motivation theory and the common in-group identity model are tested.The study results provide evidence in support of the social motivation theory:respondents who perceived Austria status as being lower than that of the other member states and who identified strongly with Austria also showed the strongest opposition to the Euro.Respondents who perceived Austria status as being equal or even higher than the status of other European states were favorable in their attitudes towards the Euro as a symbol of the union,and national identity had no main effect on their attitudes towards the Euro.

Melitski, J. (2003). "Capacity and e-government performance. An analysis based on early adopters of internet technologies in New Jersey." Public Performance & Management Review 26(4): 376-390.

This article outlines factors for public managers at the center of debates about information technology (IT) and develop a model for electronic government (e-government) implementation based on an examination of four agencies that were early adopters of Internet technologies in New Jersey state government. The agencies were selected using a Delphi technique through a survey of public managers in New Jersey State, and the data were collected through 40 semi structured interviews. The purpose is to determine the types of initiatives and investments in IT and related capacity building public agencies should emphasize to increase the performance of their e-government initiatives. This research begins by discussing seven internal IT capacity factors and then examines relevant research questions and hypotheses. Based on a content analysis of
interview transcripts, the article examines the relationship between IT capacity and e-government performance and discusses implications for further research.

Millard, J. (2003). ePublic services in Europe: Past, present and future. Research findings and new challenges, Danish Technological Institute for IPTS.

Millard, J. (2003). Progressing the Information Society: The role of government. JANUS (Joint Analytical Network for Using Socio-economic research) Workshop, Brussels.

Millard, J., J. Svava Iversen, et al. (2004). Reorganisation of government back-offices for better electronic public services – European good practices, Danish Technological Institute & Institut fὸr Informationsmanagement GmbH, University of Bremen: 188.
These are the methodological annexes of the report

Millard, J., J. Svava Iversen, et al. (2004). Reorganisation of government back-offices for better electronic public services – European good practices (back-office reorganisation), Danish Technological Institute & Institut fὸr Informationsmanagement GmbH, University of Bremen: 188.
This report presents and analyses the detailed results of one of the first studies at European level to systematically research how public agencies are using ICT to reorganise, and the impact this has upon how electronic public services are experienced by citizens and business – in other words, on the changing relationship between the front and backoffice. The study demonstrates that there is a clear and strong link between reorganising government back-offices and the electronic public services experienced by users.

Millett, L. I. and S. H. Holden (2003). "Authentication and its privacy effects." IEEE Internet Computing 7(6): 54-58.
From e-commerce to electronic tax filing to securing office building entry, the need to verify identity and authorize physical access has driven the development of increasingly advanced authentication systems. Almost all these systems use personal information (in many cases, personally identifiable information), which raises numerous privacy concerns. In early 2003, the National Academy of Sciences' Committee on Authentication Technologies and Their Privacy Implications issued a report addressing this broad set of issues. This article summarizes some of the key insights from that report.

Milne, G. R. (2003). "How well do consumers protect themselves from identity theft?" The Journal of Consumer Affairs 37(2): 388-402.
Identity theft is a serious and increasingly prevalent crime, and consumers need to take preventative measures to minimize the chance of becoming a victim. In an effort to assess consumer preparedness, this exploratory study measured the self-reported behavior of 61 college students and 59 non-students on thirteen identity theft preventative activities that were suggested by the Federal Trade Commission. Consumer education appears to be adequate for several identify theft preventative behaviors, but not for others. In addition, students and non-students demonstrated some interesting divergences in behavior. Based on these preliminary findings, areas for increased consumer education and future research are recommended.

Mitrakas, A. (2002). "Citizen centric identity management: Chip tricks." Network Security 2002(7): 15-16.

Moon, M. J. (2002). "The evolution of e-government among municipalities: Rhetoric or reality?" Public Administration Review 62(4): 424-433.
Information technology has become one of the core elements of managerial reform, and electronic government (e-government) may figure prominently in future governance. This study is designed to examine the rhetoric and reality of e-government at the municipal level. Using data obtained from the 2000 E-government Survey conducted by International City/County Management Association and Public Technologies Inc., the article examines the current state of municipal e-government implementation and assesses its perceptual effectiveness. This study also explores two institutional factors (size and type of government) that contribute to the adoption of e-government among municipalities. Overall, this study concludes that e-government has been adopted by many municipal governments, but it is still at an early

stage and has not obtained many of expected outcomes (cost savings, downsizing, etc.) that the rhetoric of e-government has promised. The study suggests there are some widely shared barriers (lack of financial, technical, and personnel capacities) and legal issues (such as privacy) to the progress of municipal e-government. This study also indicates that city size and manager-council government are positively associated with the adoption of a municipal Web site as well as the longevity of the Web site.

Mosse, B. and E. Whitley (2004). Assessing UK e-government Websites: Classification and benchmarking. European Conference of Information Systems, Turku, Finland.

Classification permeates us: our being and our world. This paper seeks to extend the information systems literature on classification by suggesting classification as a quest, involving man, in a process comprised of both finding and producing truth. Drawing on Martin Heidegger's etymological enquiry, classification is reinterpreted as a dynamic movement towards order. The essence of technology is an ordering based
on such dynamic classification. By exploring two exemplary UK governmental website benchmarking projects, our analysis identifies the means involved in producing the classifications inherent to these benchmarking projects. It further highlights the regulatory implications of dynamic classification within the information systems field.

Muffatto, M. and A. Payaro (2003). "Implementation of e-procurement and e-fulfillment processes: A comparison of cases in the motorcycle industry." International Journal of Production Economics 89(3): 339-351.

Electronic business is the process which uses Internet technology to simplify certain company processes,improve productivity and increase ef.ciency. It allows companies to easily communicate with their suppliers,buyers and customers,to integrate "back-office" systems with those used for transactions,to accurately transmit information and to carry out data analysis in order to increase their competitiveness.
The aim of this work is to define the parameters which can be used to define the performance of companies which use e-business. Particular attention is given to procurement and ful.llment in order to compare the companies studied and measure their ef.ciency. Fulfillment means controlling and managing transactions,warehouses,transportations and reverse logistics. This analysis is followed by case studies of two large Italian companies in the.field of motorcycles. The market strategy they use and the role of Information and Communication Technologies (ICT) in their procurement and distribution processes is analyzed. This comparison provides useful information regarding the way in which Internet
can be used by two companies which operate in the same market. The paper ends with the presentation of an evolutionary model for e-business strategy. The stages of the model go from the use of ICT simply as instruments of communication to the improvement of coordination processes.

Muir, A. and C. Oppenheim (2002). "National information policy developments worldwide I: Electronic government." Journal of Information Science 28(3): 173–186.

A review of recent Government initiatives in the area of e-Government based upon a review of the literature is presented. The desk research covered the period 1997 to 2001, and covered a number of major countries, including Canada, USA, Member States of the European Union, South Africa, Hong Kong, Australia and New Zealand. The UK was not included in the survey. The targets set by Government are often vague, and few governments seem to have addressed in any thoughtful manner the problems citizens might have with use of technology. An approach along the lines of 'this is bound to happen' rather than 'what sort of society do we really want?' is a common feature amongst all the approaches examined. The risks of enhancing the digital divide are also rarely explicitly addressed. Comments regarding good initiatives that offer models for other countries to adopt are made. The emergence of government portals is without doubt the most significant development. These provide the facility for personalization by the user. The New Zealand Government's efforts to ensure that its web sites are useful for citizens who have difficulty spelling and the Canadian Government's use of minority languages are also noteworthy. The leading countries are Australia, New Zealand, USA and Canada. The Australian Government's e-procurement strategy is a role model for the future.

Myhr, T. (2005). Regulating a European eID, Porvoo e-ID Group.

This document shall be used as a starting point for a discussion within the Provoo Group on what necessary steps should be taken in order to pave way for a legal framework for a pan European eID. The document is not supposed to bring all the answers but is trying to shed some light on some crucial/important questions and present some possible alternatives. The Directive on Electronic Signatures covers also entity authentication. However, entity authentication leads to special regulatory needs that are not met in the Directive on Electronic Signatures or in any other EEA relevant legal document. A legal framework for a pan European electronic ID has to be drafted with the realization of the limitations given by the EC Treaty Article 18. Given these facts the report makes the following suggestions and conclusions: - Use and interpret the existing regulation in the Directive on Electronic Signatures as far as possible as a building block for the establishment of a legal framework for a pan European electronic ID. - Take in use existing standards and promote the development of new standards for entity authentication to support the use of a pan European electronic ID. - One should maybe accept pan European electronic IDs on different security levels. It might be easier to find a consensus among Member States on a lower level. - Further evaluate the possibility to use existing national and European regulation for passports as another building block for the legal framework for a pan European electronic ID.

Neu, R., R. H. Anderson, et al. (1998). E-mail communication between government and citizens: Security, policy issues, and next steps. RAND Issue Papers. R. Corporation, RAND Corporation.

Niens, U. and E. Cairns (2003). "Explaining social change and identity management strategies new directions for future research." Theory & Psychology 13(4): 489–509.

For many years, social psychological research has tried to explain the social dynamics of intergroup conflict and individual and group differences in engagement in intergroup conflict. We argue here that, for this work to progress, a broader interpretation is required. Focusing on individual and collective identity management strategies to cope with social change, social identity theory (SIT) is reviewed and limitations of the theory are pointed out. To overcome these weaknesses in SIT, an integration of SIT with relative deprivation theory and the authoritarian personality theory is suggested. The main achievements of such an integration, we believe, would be the inclusion of a broader range of identity management strategies, clarification in relation to predictor variables and the application of identity management strategies for minority as well as majority groups.

Nilsson, O. (2003). To be, or not to be connected. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

In the debate of today concerning the Internet, e-democracy, e-governance and the private use of ICTs, Information and Communication Tools, a note of warning is often struck for 'the digital divide', 'the digital gap' or 'the digital borderline'. Whatever the expression, the intention is to pronounce the differences in access to ICTs. A main reason to pay attention to this question is the endeavour from both the public and the private sector to transform services to digital ones. The question of access to public services and information is a crucial factor both to succeed with this transformation and to fulfill the democratic values. When access to ICTs is talked about, the focus is mostly put on a physical or technical level. Conclusions concerning the use are often based on official statistics regarding the number of computers or Internet connections in a country. The problems with these conclusions, which are used to legitimise the implementation of public systems, are that they do not consider other factors among the potential users like attitude or confidence. These issues, related to the individual, are necessary to take into account in the decision process. This short paper starts from Clement and Shade's "Access Rainbow" (Clement & Shade, 2000) and suggests a direction for a study concerning driving forces and barriers related to the individual's experience of access to ICTs.

Norris, D. F. (2003). "Building the virtual state. or not? A critical appraisal." Social Science Computer Review 21(4): 417-424.

In this article, the author advances four arguments about Building the Virtual State. First, it is a historical and fails to take into account the rich and rewarding literature about information technology (IT)

and government developed over the past 3 decades. Second, its theory of IT enactment is little more than a repackaging of the dominant extant theory in the field, section systems theory. Third, evidence provided from the three case studies in the book is insufficient to test enactment (or any other) theory of IT and government. Finally, although the book claims to be about the virtual state, only one of the case studies addresses the movement of government services onto the Internet (the author's definition of the virtual state), and the other two cases do not address it at all. For these reasons, Building the Virtual State is a disappointment, and it delivers a good bit less than it promises.

O'Donnell, O., R. Boyle, et al. (2003). "Transformational aspects of e-government in Ireland: Issues to be addressed." Electronic Journal of eGovernment 1(1): 23-32.

Drawing upon Irish experience, this paper explores some of the key issues to be addressed in using e-Government effectively to transform public sector organisations. Two case studies are detailed:ROS (Revenue Online Service) and Integrated Service Centres (County Donegal). Policy implications of developments to date and remaining challenges are discussed.

Oates, B. J. (2003). "The potential contribution of ICTs to the political process." Electronic Journal of eGovernment 1(1): 33-42.

This paper discusses the potential of information and communication technologies (ICTs) to help engage people in all parts of the political process: obtaining information, engaging in deliberation and participating in decision-making. It also discusses limitations or barriers to using ICTs in these ways. Despite these limitations ICTs are likely to be increasingly tried in the political process. It is therefore important that we educate our young people for participation in an e-enabled political process. The paper therefore reports on an educational project that demonstrated using ICTs in the political process and introduced some 13-14 year olds to citizenship and electronic democracy, concentrating on a local mayoral election. The responses of the participants raise interesting issues about how to use ICTs in education and the desirability, or otherwise, of electronic electioneering. The paper contributes to our understanding and experience of citizenship education, e-democracy and the use of ICTs in the political process

OECD (2001). E-government: Analysis framework and methodology, OECD.

This paper sets out the proposed analysis framework and methodology to be adopted for the OECD e-government project. This document should be read in conjunction with PUMA(2001)10/REV2, which outlines the project parameters and working methods.

OECD (2003). The e-Government imperative. OECD e-Government Working Group, Paris, OECD Publications.

OECD (2003). The e-government imperative: Main findings. The OECD Observer, OECD.

Since the advent of computers,and more recently the Internet,pressure on governments to perform better has increased, and imformation and communication technologies (ICTs) have provided them with the capacity to do so via e government. E government is here defined as "the use of ICts, and particularly, the Internet as a tool to achive better government". The impact of e govermnet at the broadest level is simply better government– e-government is more about government than about "e". It enabled better policy outcomes, higher quality services and greater engagement with citizens. Governments and public administrations will, and should, continue to be judged against these established cirteria for success.
E-government initiatives refocus attention on a number of issues: how to collaborate more effectively across agencies to address complex, shared problems; how to enhance customer focus; and how to build relationships with private sector partners. Public administrations must address these issues if they are to remain responsive. This Policy Brief highlights policy lessons from current experience in OECD member countries and suggests 10 guiding principles for successful e-government implementation. It builds on the work of the E-Government Task Force and the OECD E-Government Working Group, and summarises the main findings of the OECD Flagship Report on E-Government "The E-Government Imperative".

OECD (2003). E-government in Finland: An assessment, OECD.

Since the 1990s, Finland has been a leader in exploiting information nd communication technology (ICT) to renew its economy and to
reform its public administration. Its reputation for successfully pro-viding proactive electronic government services and information has brought officials from around the world to learn from its experience. While Finland is an e-government pioneer, it continues to face a number of crucial e-government and broader governance challenges such as communicating a clear e-government vision and increasing inter-agency collaboration. Other challenges also include strengthening internal governance structures and ensuring owner-ship of e-government initiatives.This Policy Brief presents an assessment of e-government policies,implementation and impact in central government in Finland as part of a first comprehensive analysis of e-government implementation within the Finnish central administration. It summarises the main findings of the OECD Report E-Government in Finland, a study of e-government in the Finnish central administration carried out by the OECD E-Government Task Force with backing from the Ministry of Finance. This study takes an in-depth look at e-government structures and processes and examines their strengths and weaknesses.

Office, C. (2002). Identity fraud: A study. UK.

ID fraud is an important and growing problem linked to organized crime in a number of forms: illegal immigration (including human trafficking): money-laundering and frug running; and financial fraud against government and the private sector.
It is not easy to gauge the amount of identity fraud. But the minimum cost to the economy is in excess of £1.3bn per annum. This compares with the estimated total economic cost of all fraud of at least £13.8bn. per annum. Identity fraud is possible because of weaknesses in the processes used to issue documents used as evidence of identity, and the processes used to check identity at point of use.
Most current processes for issuing government documentation used for identity verification, and a range of unique identifying numbers, do not meet the highest private sector or overseas standards of security. Government databases are also considerably less than fully accurate, and checks on identity at point of use less than in the private sector.
Where financial fraud is concerned criminals target the public and the private sector indiscriminantly, often looking for the weakest links. But counter-fraud efforts are not similarly joined up. 'ID theft' is not in itself an offense, and penalties for those who make fraudulent applications (for example passports) are very small. Prosecutions are comparatively rare.
The private sector does not, for the most part, entirely rely on government-issued documents to check identity where its commercial interests are at stake. Rather, it checks identity against databases held by credit reference agencies which show the 'historical footprint' left by an individual in the community. the footprint is also what those legitimately developing an alias identity to work undercover find it hardest to invent, when an identity is fabricated. many private sector bodies also check applications for goods and services against a central register of frauds and fraudsters.

Oppliger, R. (2004). "Microsoft.NET Passport and identity management." Information Security Technical Report 9(1): 26-34.

As part of its.NET initiative, Microsoft developed and is currently deploying a Webbased single sign-in (SSI) service called.NET Passport. In this article, we overview, discuss, and put into perspective Microsoft.NET Passport's SSI service. More specifically, we address the question whether Microsoft.NET Passport provides an appropriate solution for the user authentication and authorization or identity management problem on the World Wide Web (WWW).

Owen, T. (1997). "Information and the taxpayer – An agenda for business." Business Information Review 14(2): 59-63.

Draws attention to the importance for business of government information and considers the business implications of recent trends towards the electronic delivery of government services. Describes the setting up of the Coalition for Public Information (CoPI) as a broad-based group that aims to address the concerns raised by these trends. Highlights the extraordinary credibility CoPI has managed to achieve and the wide support its views enjoy. Sets out the 12 policies that comprise CoPI's Manifesto for Public

Information, arguing that its proposals will be valid irrespective of which political party wins the 1997 UK general election.

Pato, J. and J. Rouault. (2003). "Identity management: The drive to federation." Technical White Papers Retrieved April, 05, 2004, from http://devresource.hp.com/drc/technical_white_papers/IdentityMgmt_Federation.pdf.
N/A

Patrick, A. S. and S. Kenny (2003). From privacy legislation to interface design: Implementing information privacy in human-computer interactions. PET Workshop pre-proceedings, Dresden.
Internet users are becoming more concerned about their privacy. In addition, various governments (most notably in Europe) are adopting strong privacy protection legislation. The result is that system developers and service operators must determine how to comply with legal requirements and satisfy users. The human factors requirements for effective interface design can be grouped into four categories: (1) comprehension, (2) consciousness, (3) control, and (4) consent. A technique called "Privacy Interface Analysis" is introduced to show how interface design solutions can be used when developing a privacy-enhanced application or service. To illustrate the technique, an application adopted by the Privacy Incorporated Software Agents consortium (PISA) is analyzed in which users will launch autonomous software agents on the Internet to search for jobs.

Patton, M. A. (2004). "Technologies for Trust in Electronic Commerce." Electronic Commerce Research 4: 9-21.
Lack of consumer trust in e-commerce merchants, e-commerce technology, and the social, financial and legal infrastructures of the e-commerce environment, poses a major challenge to the large-scale uptake of business to consumer e-commerce. Most traditional cues for assessing trust in the physical world are not available on-line. This paper gives an overview of some of the work being done to devise alternative methods for assessing, communicating and establishing trust in this environment. Examples are drawn from a wide range of disciplines including human–computer interaction, usability, marketing, information technology, mathematics, linguistics and law. Industry, self-regulatory and government initiatives aimed at building consumer trust and confidence in e-commerce are also discussed.

Peristeras, V., T. Tsekos, et al. (2002). Analyzing e-government as a paradigm shift. UNTC Occasional Papers Series. Thessaloniki, United Nations Thessaloniki Center for Public Service Professionalism.
This paper analyses e-government and attempts to show that it is a major paradigm shift in the way that government and public administration are to function. To shed light on this major breach, an analysis is performed regarding the types of information that have been produced and used by the state through time, as well as the methods employed for information processing and dissemination of information in three stages,tribal, massive and configurational. The paper reviews the effects of information technology on general organization by structuring these effects in four stages: islands of automation, automated process chains, business reengineering through IT and total reinvention. It then analyses the fourth stage as it applies to government and public administration in particular. The major changes brought upon government and public administration through IT in this fourth phase appear to have profound effects forcing even a reconsideration of what public administrations should produce and why.For this new era, an organizational, information systems and political paradigm for public administration is proposed.

Posch, R. (2003). eAustria. The Austrian view to approach e-Government, Secure Information Technology Center.

Ramanathan, S. (2004). Diffusion of e-procurement in the public sector - Revisiting centralization versus decentralization debates as a twist in the tale. European Conference of Information Systems, Turku, Finland.

Several governments are in the process of implementing e-procurement. In the process they face several challenges. The diffusion of e-procurement in the Danish public sector is researched using case study research methodology to study the challenges faced. The results of the study are applied in this paper for explaining some of the challenges faced using the legacy centralization versus decentralization debates regarding computing and organization; which forms the tale. These debates in no doubt help in kick starting the research on the diffusion of e-procurement in the public sector. However, the phenomenon under study is complex and unique in several respects that the debates alone are inadequate for fully explaining the challenges. The paper presents a question as the twist in the tale answering which helps in understanding the nature of challenges much better. The question is "To what extent is government a single organization?"

Rannenberg, K. (2004). "Identity management in mobile cellular networks and related applications." Information Security Technical Report 9(1): 77-85.

While identity management systems for the Internet are debated intensively identity management in mobile application has grown silently over the last 12 years. More then 980 million GSM subscriptions and the SIM infrastructure are the basis for many application oriented initiatives to manage identities. This paper discusses the technological foundations as well as the application scenarios and the privacy challenges and opportunities.

Rennhard, M., S. Rafaeli, et al. (2004). "Towards pseudonymous e-commerce." Electronic Commerce Research 4: 83-111.

The lack of privacy is one of the main reasons that limits trust in e-commerce. Current e-commerce practice enforces a customer to disclose her identity to the e-shop and the use of credit cards makes it straightforward for an e-shop to know the real identity of its customers. Although there are some payment systems based on untraceable tokens, they are not as widely used as credit cards. Furthermore, even without buying anything, a customer is already disclosing some information about who or where she may be by just connecting to the e-shop's web server and leaving behind an IP-address. In this paper, we present novel components that enable secure pseudonymous e-commerce. On the one hand, these components allow a customer to browse through an
e-shop, select goods, and pay the goods with her credit card such that neither the e-shop operator nor the credit card issuer nor an eavesdropper is able to get any information about the customer's identity. On the other hand, it is guaranteed that none of the involved parties is able to act dishonestly during the credit card payment. Such a system could greatly enhance trust in e-commerce since it overcomes the customers' privacy concerns.

Riedl, R. (2001). Document-based inter-organizational information exchange. The 19th annual international conference on Computer documentation, Sante Fe, New Mexico, USA, ACM Press.

In this paper,we present tour research work n d cument services for interstate e-government carried out in the FASME project.First,we depict the background for our research and we describe its basic challenges.Then we discuss the required services out f the perspective f inter-organizational document services and d cumentation issues.From the evaluations f ur prototypical implementation with user groups, we may conclude that interstate e-government services are feasible and that life without personal documents in paper form may become possible.

Riera, A. and P. Brown (2003). "Bringing confidence to electronic voting." Electronic Journal of eGovernment 1(1): 43-50.

Electronic voting (whether it is remote or poll-site) has a lack of transparency that makes its use controversial. Currently there is a lively debate regarding the deployment of electronic voting systems, with people arguing whether trustworthiness is only achievable by means of the use of backup paper trails. We believe that paper trails are not strictly necessary. In our opinion, the lack of transparency of electronic voting systems can be overcome to a great extent by using adequate security measures (technological, physical and procedural). Such security measures would provide clarity to the process and avoid the need to rely on complex and/or networked systems and/or proprietary closed systems.

Riley, T. B. and C. G. Riley (2003). E-government to e-democracy: Examining the evolution. Prepared under the auspices of the Commonwealth Secretarial and Co-sponsored Telecommunications and Informatics Program, Public Works and Government Services Canada. N. F. International Tracking Survey Report '03.

Rime, L. (2000). "Global internet trading." Card Technology Today 12(6): 12-13.
More than 20 of the world's largest banks have joined forces to remove the final obstacle to business-to-business e-commerce – trust in a trading partner's identity. To supply this trust, member banks of the Identrus group are to issue their corporate customers with smart cards to carry digital certificates that will authenticate their identity.

Robbin, A. (2001). "The loss of personal privacy and its consequences for social research." Journal of Government Information 28(5): 493-527.
This article chronicles more than 30 years of public opinion, politics, and law and policy on privacy and confidentiality that have had far-reaching consequences for access by the social research community to administrative and statistical records produced by government. A hostile political environment, public controversy over the decennial census long form, media coverage, and public fears about the vast accumulations of personal information by the private sector were catalysts for a recent proposal by the U.S. Bureau of the Census that would have significantly altered the contents of the 2000 census Public Use Microdata Sample (PUMS). These events show clearly that science does not operate independently from the political sphere but may be transformed by a political world where powerful interests lead government agencies to assume responsibility for privacy protection that can result in reducing access to statistical data.

Robiette, A. (2001). "Digital certificates and public key infrastructure." Vine 31(2): 42-49.
Digital certificates promise to provide the next major leap forward in authentication, and are in fact in use today to secure some e-commerce transactions. The paper describes what digital certificates are, what they can be used for and what the state of this technology is at present; it also discusses the problems hindering wider deployment of certificates and what needs to be done for them to gain wider acceptance.

Rohrig, S. and K. Knorr (2004). "Security analysis of electronic business processes." Electronic Commerce Research 4: 59-81.
This article introduces POSeM, a method that uses business process descriptions to derive appropriate security safeguards. This is achieved by assigning security levels to the components of a business process such as actors, artifacts, and activities with a specially developed description language. These levels are checked for consistency, and security measures are derived using a configurable rule base that maps security objectives to safeguards. POSeM in practice is illustrated by an application to electronic business, i.e., the publication process of
information for a company’s web-site. Both the advantages of POSeM and its possible refinements are discussed.

Rosen, J. (2000). The unwanted gaze: The destruction of privacy in America. New York, Random House.

Rousseau, D. M., S. B. Sitkin, et al. (1998). "Introduction to special topic forum: Not so different after all: A cross-discipline view of trust." Academy of Management Review 23(3): 393-404.
N/A

Rowe, H. (1998). "Encryption policy, securing payments through effective authentication: Evaluating trusted third party proposals for a trust hierarchy in the UK." Computer Law & Security Report 14(3): 151-158.
With the exponential growth in the use of the Internet in the past three or four years and its metamorphosis from a military and academic network to a business tool and recreational arena, the business

and user communities' attention has focused increasingly on its inherent (or perceived) weaknesses and the manner in which they can be reduced or eliminated. At the forefront of current thinking in terms of security is the use of cryptography and cryptographic techniques which can be used to ensure the confidentiality of communications, the integrity of messages and data packets and to confirm the identity of the communicating parties. Until the early 1970s, the science of cryptography was primarily of interest to governments (so that secure communications could be used by the military and intelligence services) and academic mathematicians. With the increase in the number of computer networks and uses to which they were put, security, and hence cryptographic systems, became of increasing importance to users of the systems especially in the financial services sector. However, governments (and the intelligence agencies in particular) guarded jealously the technologies in question and digital cryptographic systems were included in the list of controlled technologies produced by the Coordinating Committee for Multilateral Exports Control – – COCOM1. The approach taken by COCOM, until it was disbanded in March 1994, influences to this day the manner in which encryption technology is controlled by the United Kingdom and other European Union States. The purpose of this paper is to look at the UK Government's various proposals in relation to encryption on the public telecommunications network; it also looks at certain UK developments in relation to the use of encryption; and compares the developments in the UK with those in the EU and with some of the attitudes to the use of encryption being taken by international organizations such as the Organization for Economic Cooperation and Development (OECD) and the International Chamber of Commerce.

Rowley, T. J. and M. Moldoveanu (2003). "When will stakeholder groups act? An interest- and identity-based model of stakeholder group mobilization." Academy of Management Review 28(2): 204-219.

Using social movement and social identity theories, the authors construct a model of stakeholder group action that challenges the current notion that interests drive stakeholder group action. They argue that interests do not easily translate into action, mobilization can be motivated by a desire to express an identity as well as protect interests, and overlapping memberships across stakeholder groups affect stakeholder group action. As a result, the authors develop several propositions based on the elaboration of interest-based action and inclusion of identity-based action.

Roy, J. (2003). "Introduction e-government." Social Science Computer Review 21(1): 3-5.

The emergence of e-government may not be a natural evolution of existing public sector structures and processes, although the degree to which it is not drives much debate. Meaningful research on this topic could thus be helpful in providing a basis for more clarity, insight, and understanding of this important topic. The aim of this special issue on e-government is, as a result, to generate new and relevant scholarly contributions on the transformation at work in the public sector today, due to the growing online patterns of socioeconomic and political activity shaping individual and organizational behavior around the world.

Roy, J. (2003). "The relational dynamics of e-Government. A case study of the city of Ottawa." Public Performance & Management Review 26(4): 391-403.

The emergence of e-government unleashed a rhetorical promise perhaps unparalleled in previous phases of public sector reform. Client-centric government made possible through the advent of integrated portals, new forms of public-private partnerships, and better overall performance through the leveraging of on-line applications and new information technologies (IT) are often-heard claims. This case study presents the combined role of portals and partnerships in one segment of the transformative experience promised by the vision of e-government. Ottawa’s experience may provide insights for other governments in the process of moving on-line, and it can also be helpful in testing some of the conceptual claims put forth by both proponents and critics of e-government as a theoretical model for public sector reform.

Rycroft, R. W. (2003). "Technology-based globalization indicators: The centrality of innovation network data." Technology in Society 25: 299–317.

Useful technology-based indicators are central to efforts to gain insights into the causes and consequences of globalization. But traditional technology-based globalization indicators are of limited use because they are based exclusively on innovation inputs (e.g. R&D spending) or outputs (e.g. patenting). Coming to grips with the globalization phenomenon requires more attention to events taking place in the

innovation process itself. Indicators of technological collaboration (e.g. strategic alliances, joint ventures, intimate supplier-producer linkages) help fill this gap. Focusing on these cooperative arrangements places the emphasis where it should be¨Xon the key organizational actors (e.g. firms, universities, government agencies) in the process of globalization. Indicators based on the dynamics of these innovation networks hold great promise for integrating input and output indicators. An example is the development of indicators of social capital¨Xa stock of collective learning. Viewing globalization through the lens of the emergence and evolution of social capital points out that even in the most powerful technological innovation process, success depends as much on social factors (e.g. the key roles of trust, shared values, and community) as on economic, scientific, or engineering variables.

Saeednia, S. (2002). "An identity-based society oriented signature scheme with anonymous signers." Information Processing Letters 83(6): 295-356.

In this paper, we propose a new society oriented scheme, based on the Guillou–Quisquater signature scheme. The scheme is identity-based and the signatures are verified with respect to only one identity. That is, the verifier does not have to know the identity of the co-signers, but just that of the organization they represent.

Samarati, P., E. Damiani, et al. (2002). Multiple and dependable identity management: R&D issues.

This document discusses the problem of multiple and dependable identity management in the digital world and in emerging electronic scenarios. The document illustrates the concept of identity management and the drivers for the support of multiplicity and dependability, and provides a discussion on different research and development issues that need to be addressed toward the support of multiple and dependable identity.

Scherlis, W. L. and J. Eisenberg (2003). "IT research, innovation, and e-government." Communications of the ACM 46(1): 67 - 68.

Over the past few years, the basic outline of an e-government vision has emerged, and government has taken promising steps to deploy e-government services. Much remains to be done, however, both in implementing e-government services and in developing new technologies and concepts, if the e-government vision is to be broadly realized. A recent study by the National Research Council's Computer Science and Telecommunications Board [2] examines several aspects of this challenge. It identifies areas where government is a demand leader for IT, explores the roles of IT researchers in risk-managed e-government innovation, and discusses approaches that can help accelerate innovation and foster the transition of innovative technologies from the lab to operational systems.

Schultz, E. (2002). "The gap between cryptography and information security." Computers and Security 21(8): 674-676.

Few controls available to information security professionals today are more potentially powerful than is encryption. Among the many important benefits of encryption are data confidentiality, integrity of data and system files, protection against repudiation in business and other transactions, assurance of individuals' identity, protection against cheating in voting and contract signing, and others. Security professionals are required to know at least the basics of cryptography to pass professional certification tests such as the CISSP exam; they must often know much more to be able to be proficient on the job. A number of vendors have produced impressive encryption products for desktop encryption, authentication methods, virtual private networks (VPNs), and digital signatures. Significant advances in cryptography and cryptanalysis research have also occurred over the years.

Schware, R. and A. Deane (2003). "Deploying e-government programs: the strategic importance of "I" before "E"." The Journal of Policy, Regulation and Strategy for Telecommunications 5(4): 10-19.

Many developing countries are in the initial phases of adopting electronic government (e-government) programs to improve public services and deliver them as efficiently and conveniently as possible. Our experience with a variety of governments throughout the developing world at different stages

of implementing e-government programs with citizens (G2C), businesses (G2B), and other entities of government (G2G) suggests that a major reason behind the success or failure of e-government projects is the extent to which, first, the governments address technological infrastructure encouraged by appropriate telecommunications policies; and second, the legal and regulatory instruments required for e-government. Information and communication technology (ICT) infrastructure (the "I") development is at the heart of successful deployment and sustainability of e-government programs.

Schwuchow, W. (1999). "The role of government in the information society: lessons from Germany." Business Information Review 16(2): 96-106.

In view of the turbulent development of electronic information markets one could - rashly perhaps - arrive at the conclusion that this area of economic activity could without hesitation be left to the operation of market forces (supply and demand). But is this really the case? Have important social and wider aspects not been taken into consideration? In order to put this question into its historical context, the development of national information policy over the past 30 or 40 years will be outlined. Taking accepted criteria used in fiscal science, consideration will be given to which part of information provision could be organized most efficiently on a free enterprise basis and in which part of this sector of the economy the state has to accept some responsibility. A responsibility which extends beyond merely creating the framework conditions for the functioning of a free enterprise system. Finally, from these fiscal science criteria, different phases of German information policy will be examined critically under the magnifying glass, from the beginning of the 1960s to date (up to 1990 those of the then German Federal Republic).
This article is based on a paper given at the International Conference 'Information Provision - Policy and Strategy' 28 June-July 1998 at the
Frankenwarte Academy, Wurzburg (Germany).

Scott, M., W. Golden, et al. (2004). A click and bricks strategy for egovernment. 17th Bled eCommerce Conference, eGlobal, Bled, Slovenia.

Two of the central challenges of e-government are the need for 'joined-up' government through agency collaboration, and the need to provide 'citizen-centred' government, where services and information are integrated at the point of delivery. Electronic service delivery provides the hoped for panacea to enable not only administrative efficiencies in the functions of government, but also services that are centred on the needs of the citizen. The implementation of e-government however, presents challenges regarding the achievement of inter-agency collaboration and highlights the importance of developing multiple access channels. This paper reports from an in-depth case study detailing first, the strategy the Irish government adopted for electronic service delivery and second, provides detailed analysis from the pioneering efforts of an individual county council into agency collaboration and a unique method of service provision. Two survey questionnaires conducted with staff of the county council and citizens of the county, reveal critical success factors in developing inter-agency collaboration and raise important concerns expressed by citizens into data privacy, social inclusion and the digital divide.

Seifert, J. W. and R. E. Petersen (2002). "The promise of all things E? Expectations and challenges of emergent electronic government." Perspectives on Global Development and Technology 1(2): 193-212.

The ambiguous nature of electronic government (e-government) has resulted in hype and confusion, with little systematic consideration of the expectations and limitations of taking government online. This paper seeks to examine the role of e-government in the United States as an evolving process that manifests itself in three distinct sectors: government-to-government, government-to-business, and government-to-citizen. Using this typology as an organizing principle, we show how information technology has the potential to enhance government accessibility and citizen participation. We also show how the move toward a market-focused conceptualization of government information and service delivery raises the potential for blurring citizen and consumer roles, possibly at the cost of a robust, informed, and engaged citizenry

Simpson, P. and X. Huang (2002). "Success at e-governing: A case study of ESDLife in Hong Kong." Electronic Markets 12(4): 270-280.

Slosarik, K. (2002). "Identity theft: An overview of the problem." The Justice Professional 15(4): 329-343.

Identity theft is becoming prevalent and increasing problem within the United States. An identity thief only needs one thing - a Social Security Number; with it, he can decimate a victim's life and credit. Historically, federal laws in place to combat identity theft are weak and ineffective. Law enforcement, faced with jurisdictional and technological issues, is ill-equipped to deal with this. State and local law enforcement are forced to look to numerous federal agencies for help in combating this crime. It is difficult to determine the scope of this problem but initial figures show that identity theft has many different types of victims and financial targets. The ways in which identity thieves victimize and prevention practices individuals can use to protect themselves are also examined. This article establishes a literature review on which future, and much needed, research can be based.

Smith, R. E. (2000). Ben Franklin's web site: Privacy and curiosity from Plymouth Rock to the Internet. Providence, Privacy Journal.

The book describes Puritan monitoring in Colonial New England, then shows how the attitudes of the founders placed the concept of privacy in the Constitution. This panoramic view continues with the coming of tabloid journalism in the Nineteenth Century, and the reaction to it in the form of a new right – the right to privacy. The book includes histories of wiretapping, of credit reporting, of sexual practices, of Social Security numbers and ID cards, of modern principles of privacy protection, and of the coming of the Internet and the new challenges to personal privacy it brings

Sniderm, J. H. (2003). "Should the public meeting enter the information age?" National Civic Review 92(3): 20 - 29.

Solow, J. L. and N. Kirkwood (2002). "Group identity and gender in public goods experiments." Journal of Economic Behavior & Organization 48: 403-412.

This paper explores the effects of group identity and gender in a public goods experiment.We compare the behavior of participants who can be expected to have a pre-existing sense of group identity to that of randomly selected participants,and to that of participants who have undertaken community-building pre-experiment activities.While statistically significant differences were observed,our results suggest that the effects of group identity and gender on behavior are complicated, involving the nature of the groups involved.In particular,the claim that women are less likely to free-ride on others with whom they have a relationship is not supported.

Sondheimer, N. K., L. P. Osterweil, et al. (2003). E-government through process modeling: A requirements field study. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

e-Government offers its constituency the hope of engaging in government interaction at any time from any place. This has been slow to materialize. We believe this is due in large part to the complexity of government processes. This paper reports experimental field study evidence that a rigorously defined process modeling language can accurately map this complexity. It introduces Little-JIL, a rigorously defined process modeling language. It then reports experience using this language to capture government processes for an e-Government system to allow online license renewals for the government of Massachusetts. These processes were previously described using Use Case methodology. The errors and shortcomings identified provide opportunities for a more correct and efficient implementation of these processes. The paper concludes with a proposal for improved e-Government development methods.

Sorrentino, M. (2004). The implementation of ICT in public sector organisations. Analysing selection criteria for e-government projects. 17th Bled eCommerce Conference, eGlobal, Bled, Slovenia.

Taking as a starting point the recent approval of 138 co-financing proposals put forward by numerous Italian public bodies within the context of a national e-government plan, the article poses the

question of whether these types of initiatives are really likely to unleash mechanisms capable of improving organisational performance. The evaluation criteria adopted in the course of the selection process are analysed on the basis of a model elaborated by Soh and Markus (1995). The aims are: to carry out a general assessment of the role attributed to information and communication technology (ICT) in the modernization of the public sector and to draw some conclusions from this progress towards the realization of e-government.

Spencer, S. (2003). Ubiquitous e-government. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

Providing access to government information and services to citizens via the Internet has emerged as a key component of e-Government. Broad objectives of demonstrating leadership in the Information Society and improving citizen access, while restraining or reducing costs, are well understood and have global relevance. However, local implementation with resource constraints, limited experience and limited awareness has challenged policy makers and managers. This paper reviews strategies applied by Australian governments at national and state levels. From a proposed typology of policy approaches, effectiveness of strategies for encouraging participation of government agencies can be examined. It is argued that the objectives of maximum participation and maximum effectiveness, particularly through online integration of services, cannot be dealt with simultaneously.

Spiekermann, S., J. Grossklags, et al. (2001). E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. Third ACM Conference on Electronic Commerce, Tampa, Florida, US.

As electronic commerce environments become more and more interactive, privacy is a matter of increasing concern. Many surveys have investigated households' privacy attitudes and concerns, revealing a general desire among Internet users to protect their privacy. To complement these questionnaire-based studies, we conducted an experiment in which we compared self-reported privacy preferences of 171 participants with their actual disclosing behavior during an online shopping episode. Our results suggest that current approaches to protect online users' privacy, such as ECU data protection regulation or P3P, may face difficulties to do so effectively. This is due to their underlying assumption that people are not only privacy conscious, but will also act accordingly. In our study, most individuals stated that privacy was important to them, with concern centering on the disclosure of different aspects of personal information. However, regardless of their specific privacy concerns, most participants did not live up to their self-reported privacy preferences. As participants were drawn into the sales dialogue with an anthropomorphic 3-D shopping bot, they answered a majority of questions, even if these were highly personal. Moreover, different privacy statements had no effect on the amount of information disclosed; in fact, the mentioning of EU regulation seemed to cause a feeling of 'false security'. The results suggest that people appreciate highly communicative EC environments and forget privacy concerns once they are "inside the Web".

Spinello, R. A. (2002). Regulating cyberspace: The policies and technologies of control. Westport, CT, Quorum Books.

Sproule, C. M. (2002). "The effect of the USA Patriot Act on workplace privacy." The Cornell Hotel and Restaurant Administration Quarterly 43(5): 65-73.

Legal protections for employees against surveillance exist, but so, too, do lawful provisions for employers and government agencies to monitor employees' workplace activities—especially in the aftermath of 9/11 and passage of the USA Patriot Act.

Stafford, T. F. (2003). "E-services." Communications of the ACM 46(6): 26-28.

As I sit here considering how to introduce this special section on e-services, I'm reminded of a superb experience I recently had filing my U.S. federal income tax return. In lieu of a $400 fee for paying someone to prepare my modestly complex 2002 financial circumstances, and having moved to a new state far from my long-time accountant, I decided to take a chance on one of the new tax filing services available online.

This would be, in fact, my first substantial e-services experience as a consumer. Given I was dealing with the Internal Revenue Service (IRS), and the fact that thousands of dollars were at stake, it was no mere exercise to me.

Stalder, F. (2000). Digital identities patterns in information flows. Budapest, Intermedia Departement, Academy of Fine Arts.

Identity is, in large parts, dependent on communication. What one can be and what can be one is determined in interaction. If this interaction takes place through communication media, it consists primarily of exchanges of information. The shapes of such identity-building exchanges are molded by the media in which they take place. If these media change, then the possible and actual shapes of identity change with them. This essay explores the conceptual framework of informational identity in regard to some the emerging shapes developed by cultural activists within interactive media environments. But first, a flash back.

Stalder, F. (2000). "Informational identity: From analog to digital." Korunk Retrieved February, 11, 2004, from http://felix.openflows.org/html/id_ana_dig.html.

Stalder, F. (2002). "Opinion. Privacy is not the antidote to surveillance." Surveillance & Society 1(1): 120-124.

Stalder, F. and D. Lyon (2002). Electronic identity cards and social classification. Surveillance as social sorting: Privacy, risk and automated discrimination. D. Lyon, Routledge: 137-172.

Statskontorent and The Swedish agency for administrative development (2000). The 24/7 agency. Criteria for 24/7 agencies in the networked public administration.

Statskontorent and The Swedish agency for administrative development (2002). Interconnected government. A proposal for strengthening central co-ordination of e-government development efforts.

Steyaert, J. (2000). "Local governments online and the role of the resident. Government shop versus electronic community." Social Science Computer Review 18(1): 3-16.

This article explores the ways municipalities use the Internet as a new medium to interact with residents. Many local governments develop new tools to serve citizens' needs for information, services, and participation. The Internet is developing fast as a means to realize all this at once, in one "place." In Flanders, Belgium, there is a trend in electronic services for the government to reduce the citizen to a customer. Such important civic roles as being a voter and being a contributor to policy making are reduced to a minimum. Consequently, local government web sites are primarily one-way streams to the citizen as customer. The interactive possibilities of municipal web sites are neglected. This holds the risk that in future, local authorities will (voluntarily) neglect the democratic possibilities the Internet offers. In this way, they are developing an electronic government shop rather than the electronic community that some have predicted.

Steyaert, J. C. (2004). "Measuring the performance of electronic government services." Information & Management 41(3): 369-375.

The World Wide Web (WWW) and the Internet have streamlined government information, products, and services. Electronic government now includes on-line filing of documents, notification of entitlements, permits, registration, and disaster relief. This paper addresses the question, can a marketing model be used by Federal and state agencies to improve the content and value of electronic services to the public? Six Federal and state e-service programs were analyzed—the National Institutes of Health (NIH), the US Mint,

the Internal Revenue Service (IRS), the US Postal Service (USPS), and the e-State-government systems of California and New Jersey. Five marketing indicators were used—consumer awareness, popularity, contact efficiency, conversion, and retention. Awareness deals with the number of visitors to a site. Popularity refers to the rank of the site. Contact efficiency indicates site usability and content. Conversion refers to customer satisfaction, transactions and time on the site. Retention deals with customer loyalty.Web traffic reports and customer surveys were used as proxies to analyze and compare a sample of Federal and state e-service agencies. The results support the use of a marketing framework in organizing and evaluating these sites. The case studies demonstrate how statistical and survey data were combined for a robust assessment of the e-services.

Stirland, M. (2000). "Identrus — the 'Technical Platform'." Information Security Technical Report 5(4): 84-89.

In his outline of Identrus, John Bullard described the business rationale for its existence, and its fundamental principles of trust, global interoperability and simplicity. He has explained how the delivery of identity assurance services, within a supporting framework of operating rules, and governed through the application of private contract law, allows Identrus to deliver trusted digital signature services on a global basis. In this article we discuss how these services are realized by Identrus and its participants, in practice, and outline some of the technology underpinning the system.

Stott, C. and J. Drury (2000). "Crowds, context and identity: Dynamic categorization processes in the 'poll tax riot'." Human Relations 53(2): 247–273.

Reicher has recently developed the social identity model of crowd behaviour based on self-categorization theory (SCT). This model begins to tackle the thorny theoretical problems posed by the dynamic nature of crowd action (Reicher, 1996b). The present paper describes an ethnographic study of a crowd event in which there were changes in the inter-group relationships over time. It is suggested that the laboratory evidence in support of SCT is complemented by ethnographic research of this type. By exploring situations in which definitions of context and/or categories are not purposefully manipulated, we can demonstrate the explanatory power of a dynamic and interactive approach to social categorization.

Stratford, J. (2002). "Computerized and networked government information column." Journal of Government Information 29(5): 285-292.

The USA Patriot Act has raised concerns about its implications for Americans' rights and freedoms and has been widely criticized by civil rights and privacy groups. This column focuses on the enhanced surveillance authorities under the new law.

Stratford, J. S. and J. Stratford (2000). "Computerized and networked government information." Journal of Government Information 27(5): 595-599.

1. United States online privacy initiatives 2. Restrictions on Internet access to information on hazardous waste sites 3. Sampling controversy resurfaces at census

Stratford, J. S. and J. Stratford (2001). "Computerized and networked government information carnivore." Journal of Government Information 28(1): 109-112.

Strath, B. (2002). "A European identity: To the historical limits of a concept." European Journal of Social Theory 5(4): 387–401.

A European identity is an abstraction and a fiction without essential proportions. Identity as a fiction does not undermine but rather helps to explain the power that the concept exercises. The concept since its introduction on the political agenda in 1973 has been highly ideologically loaded and in that capacity has been contested. There has been a high degree of agreement on the concept as such, but deep disagreement on its more precise content and meaning. The concept of a European identity is an idea expressing contrived notions of unity rather than an identity in the proper sense of the word and even takes

on the proportion of an ideology. In this sense the concept is inscribed in a long history of philosophical and political reflection on the concept of Europe. On these grounds the analytical use of 'identity' in social sciences can be questioned.

Strejcek, G. and M. Theil (2003). "Technology push, legislation pull? E-government in the European Union." Decision Support Systems 34(3): 305-313.

E-government is new on the European agenda. Member states have announced plans to a more open, accessible and transparent administration by using the latest in information technology. Yet, the current situation is far from that. Hardly coordinated projects and the notorious individualism of the member states probably describe the state of affairs best. The paper assesses the status quo of e-government in the European Union and explains the current problems by missing coordination in legislature.

Stuart, E. (2003). "Plague, panopticon, police." Surveillance & Society 1(3): 240-253.

This article resituates the Panopticon in Foucault's work, showing how it emerged from research on social medicine in the early to mid 1970s, and relating it to discussions of the plague and the police. The key sources are lectures and seminars from this period, only partly translated in English. What is of interest here is how Foucault's concerns with surveillance interrelate with concerns about society as a whole – not in thetotal institution of the prison, but in the realm of public health. This is pursued through detailed readings of Foucault's analyses of urban medicine and the hospital. The article closes by making some general remarks about situating Foucault's books in the context of his lecture courses, and about how the analysis of medicine may be a more profitable model for surveillance than the Panopticon.

Sveningsson, S. and M. Alvesson (2003). Managing managerial identities: Organizational fragmentation, discourse and identity struggle. Institute of Economic Research Working Paper Series. S. o. E. a. Management. Lund, Lund University: 22.

The study is a case study of managerial identity work, based on an in-depth case of a senior manager and the organizational context in which she works. The paper addresses the interplay between organizational discourses, role expectations, narrative self-identity and identity work. Identity is conceptualized in processual terms as identity work and struggle. The paper illuminates fragmentation as well as integration in the interplay between organizational discourses and identity. It aims to contribute to a processual oriented identity theory and to the methodology of identity studies through showing the advantage of a multi-level intensive study

Swedberg, D. and J. Douglas (2003). "Transformation by design: An innovative approach to implementation of e-government." Electronic Journal of eGovernment 1(1): 43-50.

A new approach is emerging for implementing e-Government. That approach draws on lessons learned by both "dot.coms" and brick-and-mortar (government and commercial) institutions in addressing challenges of the Digital Economy to enable "transformation by design". "Transformation by design" marries a step-by-step approach to changing existing business infrastructure with innovation to accelerate progression toward transformation in the Digital Economy. In doing so, it addresses the competing requirements facing government institutions for simultaneous incremental and radical change posed by e-Government implementation.

Sykes, C. J. (1999). The end of privacy: Personal rights in the surveillance society. New York, St. Martin's Press.

Tam, M. K. W. and K.-F. Wong (2003). Web-services for e-government – A marriage for interoperability. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

eGovernment is an exciting area for applying Information and Communication Technologies (ICT). ICT can improve the efficiency and effectiveness in the provision and delivery of citizen services. A critical issue for the eGovernment implementation is the interoperation problem among heterogeneous legacy

government systems. In this aspect, the universal system interoperability supported by the XML-based webservices technologies can be an useful components in a holistic eGovernment infrastructure. In this short paper, we review the specific requirements for the webservices infrastructure in the government domain. Based on this, a number of webservices models that are appropriate for the eGovernment infrastructure are presented.

Tambouris, E. and E. Spanos (2002). "An architecture for integrated public service delivery based on life-events." Electronic Markets 12(4): 281-288.

One-stop government refers to the integration of public services from a citizen's – or customer of public services – point of view. In this paper, a life-oriented framework to realizing one-stop government is presented. The proposed framework consists of three layers: the front-office that
includes a portal where services are provided in the concept of life events; the back-office where core processes are performed; and the mid-office where life events are correlated with core processes. The resulting architecture enables each public authority to define authority-related
life events by integrating its own public services and to provide these life events via its portal. It also enables a central authority to define life events by integrating core processes performed at different public authorities and provide these life events via a central portal.

Tan, C. W. and S. L. Pan (2003). "Managing e-transformation in the public sector: An e-government study of the Inland Revenue Authority of Singapore (IRAS)." European Journal of Information Systems 12(4).

Tan, C. W. and S. L. Pan (2005). "Managing stakeholder Interests in e-government implementation: lessons learned from a Singapore
e-government project." Journal of Global Information Management 13(1): 31-53.

As e-government plays an increasingly dominant role in modern public administrative management, its pervasive influence on organizations and individuals is apparent. It is, therefore, timely and relevant to examine e-governance—the fundamental mission of e-government. By adopting a stakeholder perspective, this study approaches the topic of e-governance in e-government from the three critical aspects of stakeholder management: (1) identification of
stakeholders; (2) recognition of differing interests among stakeholders; and (3) how an organization caters to and furthers these interests. Findings from the case study point to the importance of (1) discarding the traditional preference for controls to develop instead a proactive attitude towards the identification of all relevant collaborators; (2) conducting cautious assessments of the technological restrictions underlying IT-transformed public services to map out the boundary for devising and implementing control and collaboration mechanisms in the system; and (3) developing strategies to align stakeholder interests so that participation in e- government can be self-governing.

Terry, D. J. (2003). "Social identity and diversity in organizations." Asia Pacific Journal of Human Resources 41(1): 25-35.

In this paper, a social identity perspective on the management of diversity in organizations is outlined. The perspective is well-placed to offer considerable insight in this area, given that it explicates the processes through which group memberships impact on people's attitudes and behavior both within and between groups that are operative in the workplace. According to this perspective, relative group status and the perceived permeability of intergroup boundaries are key factors that need to be considered in any efforts to understand intergroup relations
in the workplace. After a brief overview of the social identity perspective, the paper discusses: 1) the role that group status and perceived permeability play in determining the nature of intergroup relations in the workplace, and 2) the type of interventions that can be derived from a social identity perspective in an effort to improve intergroup relations in the workplace.

Timmers, P. (2004). eGovernment - Taking COMO forward. Information Society Directorate-General. The European Commissions, European Commission: 3.

Tsai, W. and S. Ghoshal (1998). "Social capital and value creation: The role of intrafirm networks." Academy of Management Review 41(4): 464-476.

Using data collected from multiple respondents in all the business units of a large multinational electronics company, the authors examined the relationships both among the structural, relational, and cognitive dimensions of social capital and between those dimensions and the patterns of resource exchange and product innovation within the company. Social interaction, a manifestation of the structural dimension of social capital, and trust, a manifestation of its relational dimension, were significantly related to the extent of interunit resource exchange, which in turn had a significant effect on product innovation.

Tsakalidis, A., P. Markellou, et al. (2003). E-government and applications levels: Technology at citizen service. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

Nowadays, more and more governments all over the world are trying to change their traditional profile to an electronic one. E-government aims at providing better and quicker services from the public services, not only to citizens but to enterprises as well. However, e-government's successful development and operation demands proper design, which will comprise the basis for its application. This adaptation can be implemented gradually in levels, which will enable the unobstructed data flow from/to public sector and will give the opportunity to citizens and enterprises to obtain the highest access to the services that are provided by the state. This paper presents the application levels of e-government from the lowest one to the highest and more complicated one.

Tsang, A. K. T., H. Irving, et al. (2003). "Negotiating ethnic identity in Canada. The case of the "Satellite Children "." Youth & Society 34(3): 359-384.

Satellite children are children of ethnically Chinese immigrants to North America who have returned to their country of origin after immigration. Based on interview transcripts of 68 adolescent satellite children,an analysis on the negotiation of ethnic identity was performed using the NUD*IST software.The analysis showed multiple ways of ethnic identity negotiation,ranging from an essentialist approach to differentiation and to confusion.Existing approaches to theoretical conceptualization are critically examined,drawing implications for practice.

Tzeng, S.-F. and M.-S. Hwang (2003). "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem." Computer Standards & Interfaces 26: 61–71.

In this article, we shall adopt the concepts of elliptic curve cryptosystems and self-certified public keys to build a novel digital signature scheme with message recovery. The public key and the identity of the user can be authenticated simultaneously in recovering the message. In addition, we shall also present three extended digital signature schemes based on the proposed scheme. The first is an authenticated encryption scheme that only allows a designated verifier to retrieve and verify the message. The second is an authenticated encryption scheme with message linkages used to deliver a large message. And the third is for message flows. The authenticated encryption scheme with message linkages for message flows allows the verifier to recover partial message blocks before obtaining the whole signature. Some possible attacks will be considered, and our security analysis will show that none of them can successfully break any of the proposed schemes.

Vasireddy, R., S. Wolter, et al. (2004). "Security posture for civilian and non-civilian networks." Bell Labs Technical Journal 8(4): 187 - 202.

Network security is dependent upon securing individual components, services, and applications. This is done through the prevention, detection, and correction of threats and attacks that exploit ulnerabilities in the network. Network security must be analyzed using various factors, such as security requirements, the inherent strengths and vulnerabilities of different network technologies, and the processes used to design, deploy, and operate networks. The Bell Laboratories security model provides the framework required to plan, design, and assess the end-to-end security of networks. In this paper, the Bell Labs security model is

used to (1) define the basic security needs of civilian and non-civilian networks, (2) examine the security capabilities of various technologies and identify their security strengths and gaps, (3) identify key threat-mitigation strategies for civilian and non-civilian networks, and (4) illustrate the value of a comprehensive framework (e.g., the Bell Labs model) in any security program, whether designed for a civilian or a non-civilian network.

Vassilakis, C., G. Lepouras, et al. (2004). "Integrating e-government public transactional services into public authority workflows." Electronic Government 1(1): 49-60.

Documents submitted by citizens through electronic services, deployed in the context of e-government, must usually undergo processing by some organisational information system in order to complete the citizens' requests and for the reply to be returned to the citizen. The integration, however, of the e-service delivery platform and the organisational information system is often hindered for a number of reasons, including security considerations, platform diversity or idiosyncrasies of legacy information systems. In this paper, we present a generic method for providing seamless communication between the two platforms, enabling the full integration of documents submitted through electronic services into the organisational workflow, thus leveraging the quality of services offered to citizens and facilitating e-service development and operation.

Vaz, P. and F. Bruno (2003). "Types of self-surveillance: From abnormality to individuals 'at risk'." Surveillance & Society 1(3): 272-291.

The major objective of this article is to inquire into the kind of subjectivity produced by surveillance practices. The analysis begins by questioning a certain understanding, widespread in the literature of new surveillance technologies, of Foucault's conceptions of power and surveillance. In brief, this understanding privileges the surveillance of many by few, of 'us' by 'them'. We contend, instead, that Foucault stressed in diverse books and articles the nexus between power relations and practices of the care of the self. Hence, techniques of surveillance are necessarily related to practices of self-surveillance. This theoretical framework constitutes the basis for differentiating two historically distinct types of self-surveillance: the first, proper to disciplinary society, is promoted by normalizing power; the second is associated to the increasing relevance of the epidemiological concept of risk in the problematizing of health-related behaviors. Epidemiology of risk factors, medical testing and genetics are opening up a temporal gap between the diagnostic of illnesses/diseases and their subjective symptoms. This gap is equivalent to a space for individual 'pre-emptive' action against possible illnesses/diseases.

Verbeek, J. P. G. M. and S. M. H. Kenny (2002). Cyber crime and data protection in the internet era. Brusseles, Institute for Knowledge and Agent Technology (IKAT),University Maastricht.

Waddell, P. and A. Borning (2004). "A case study in digital government: Developing and applying UrbanSim, a system for simulating urban land use, transportation, and environmental impacts." Social Science Computer Review 22(1): 37-51.

The UrbanSim project provides a case study in Digital Government, and this article examines progress to date in developing and applying the system in a range of metropolitan areas. Digital Government is meant here in the context of an innovative, cross-cutting initiative of the National Science Foundation. The project integrates academic research on urban simulation modeling and policy evaluation with research on human-computer interaction and software engineering, and uses a value-sensitive design to ensure that the system addresses the needs of governments and citizens. This article addresses the importance of the problem domain and the project objectives, presents a range of challenges, and outlines the design and application of UrbanSim in response to these. It discusses issues arising in the application of the model in the Salt Lake City metropolitan region, where a lawsuit over a highway project has precipitated use of UrbanSim to assess the interactions of transportation, land use, and environmental outcomes, and concludes with an assessment and directions for future research.

Wang, S., S. E. Beatty, et al. (2004). "Signaling the trustworthiness of small online retailers." Journal of Interactive Marketing 18(1): 53-69.

One of the major challenges facing all online retailers, especially small online retailers, is how to initiate consumer trust. This study examines the nature of this unique type of consumer trust by proposing the concept of cue-based trust. It also examines the signaling role of various cues in building initial trust and the behavioral consequences involved. A 25-1 factorial experiment was conducted with sample size of 402 to explore the signaling effects of five cues of interest in this study: seals of approval, return policy, awards from neutral sources, security disclosures, and privacy disclosures. The online study supported the signaling roles of most of these cues. Findings can be summarized as follows: (a) security disclosures and awards from neutral sources were found to enhance cue-based trust which, in turn, positively influenced two behavioral responses - bookmarking intentions and willingness to provide personal information, and (b) seals of approval and privacy disclosures were found to directly encourage consumers' willingness to provide personal information while awards from neutral sources were found to directly encourage bookmarking intentions. Implications for online retailers and future theoretical studies are discussed.

Weare, C., J. A. Musso, et al. (1999). "Electronic democracy and the diffusion of municipal web pages in California." Administration & Society 31(1): 3-27.

Although the Internet has been touted as a means to improve democratic governance, there has been little systematic analysis of its use. The authors analyze the diffusion of municipal Web sites that include information concerning a specific locality. The analysis is based on demographic and fiscal data from 454 California cities and two surveys of Web site adoption. The authors' theoretical framework draws from the political economy and technology diffusion literatures. City size, government resources, concentration of social-economic elites, and voter registration levels are the most significant predictors of adoption. In contrast to previous adoption studies, the authors find that liberal political ideology and experience with advanced communication technologies do not appreciably increase the probability of adoption.

West, D. M. (2002). State and federal e-government in the United States, Center for Public Policy Brown University.

This report presents the third annual update on the features that are available online atAmerican state and federal government websites. We examine the differences that exist across the 50 states and between the state and federal governments as well as compare the Summer,2002 results to 2000 and 2001. Using a detailed analysis of 1,265 state and federal government websites, we measure what kinds of features are available on-line, what variations exist across the country as well as between state and national government sites, and how e-government sites respond to citizen requests for information.In general, we find several interesting changes from past years. In the post-September 11 world, governments are taking security and privacy much more seriously than they did in 2000 and 2001. More public sector websites publish security policies on their sites, and there has been an increase in the percentage that publicize their privacy policies as well. However, this attention to security also has led to an increase in the presence of "restricted areas" on government websites that require registration and passwords for entrance (plus occasionally premium payments). Governments are creating restricted areas for a variety of reasons, such as an interest in providing premium services, a greater focus on security, personalized service delivery, and bidding on public contracts. But as we discuss later in this report, these developments are encouraging the creation of a "two-class" society in regard to e-government. Rather than
providing free and open access to all parts of electronic governance, government websites now contain restricted areas and sections requiring premium fees or subscriptions to gain access.These developments raise problems for the future of e-government. Among the more important findings of the research are:
1) there are high levels of access to publications (93 percent) and data bases (57 percent)
2) of the websites examined this year, 23 percent offered services that were fully executable online, about the same as the 25 percent that had online services last year
3) the most frequent services were filing taxes online, applying for jobs, renewing driver's licenses, and ordering hunting and fishing licenses online
4) a growing number of sites are offering privacy and security policy statements. This year, 43 percent have some form of privacy policy on their site, up from 28 percent in 2000. Thirty-four percent now have a visible security policy, up from 18 percent last year

5) Twenty-eight percent of government websites have some form of disability access, up slightly from 27 percent last year
6) seven percent of sites offered any sort of foreign language translation feature, up slightly from the 6 percent we found last year
7) six percent of government websites had restricted areas and one percent have premium features requiring payment for access
8) states vary enormously in their overall ranking based on web presence. Tennessee, New Jersey, California, Connecticut, Pennsylvania, Texas, Washington, Nevada, South Dakota, and Utah ranked highly while Wyoming, Alabama, Mississippi, and Colorado did more poorly
9) in terms of federal agencies, top-rated websites included those by the Federal Communications Commission, Department of Labor, Environmental Protection Agency, Department of Treasury, Department of State, Social Security Administration, and FirstGov (the national government portal), while U.S. circuit courts and the Supreme Court had the lowest ranking sites.
10) in general, federal government websites did a better job of offering information and services to citizens than did state government websites
11) government officials were not as responsive this year as was the case last year in terms of responding to email queries. Whereas 80 percent answered our sample query last year, only 55 percent did this year.

West, D. M. (2004). "E-government and the transformation of service delivery and citizen attitudes." Public Administration Review 64(1): 15-27.

The impact of new technology on public-sector service delivery and citizens' attitudes about government has long been debated by political observers. This article assesses the consequences of e-government for service delivery, democratic responsiveness, and public attitudes over the last three years. Research examines the content of e-government to investigate whether it is taking advantage of the interactive features of the World Wide Web to improve service delivery, democratic responsiveness, and public outreach. In addition, a national public opinion survey examines the ability of e-government to influence citizens' views about government and their confidence in the effectiveness of service delivery. Using both Web site content as well as public assessments, I argue that, in some respects, the e-government revolution has fallen short of its potential to transform service delivery and public trust in government. It does, however, have the possibility of enhancing democratic responsiveness and boosting beliefs that government is effective.

Westen, T. (2003). "E-democracy: Ready or not, here it comes." National Civic Review 89(3): 217 - 228.

Whitson, T. L. and L. Davis (2001). "Best practices in electronic government: Comprehensive electronic information dissemination for science and technology." Government Information Quarterly 18(2): 79-91.

The Department of Energy's (DOE) Scientific and Technical Information Program (STIP) has successfully reinvented the way in which DOE collects, organizes, archives, disseminates, and uses scientific and technical information in the performance of research and development (R&D). Through a suite of innovative Web-based products conceived and developed by the Department's Office of Scientific and Technical Information (OSTI), information and resources resulting from the Department's R&D activities, as well as worldwide information needed by the research community, are readily available to all users in a fully integrated E-Government environment. This suite of products is accessible publicly at,http://www.osti.gov.

Wild, R. H. and K. A. Griggs (2004). "A web portal/decision support system architecture for collaborative intra-governmental planning." Electronic Goverment 1(1): 61-76.

In this paper, we focus on the US intra-governmental initiative to improve internal efficiency and effectiveness (IEE) using information technology. We propose a web portal architecture that permits government planning teams to collaborate in an effective way to make more informed and better decisions. The architecture incorporates a simulation decision support system, which provides remote teams with the ability to experiment with a variety of planning scenarios to gain an understanding of the effects of policies and rules on team coordination and overall performance. The web portal architecture allows government agencies to share simulation results and discuss potential plans before implementing them.

Wilsher, R. G., M. S. Baum, et al. (2000). Achieving global trust in an e-world. 23rd National Information Systems Security Conference, Baltimore, MD. USA.

The NISSC has a long and respected heritage as an important event in the field of information security. Its origins lie in the defense arena, which has naturally been subject to a very national perspective. However, in recent years the influence of 'infosec' has spread pervasively into the commercial domain; in that time its scope has also become fundamentally international. This panel has come about because its members believe that it is appropriate for the NISSC to adopt now a broader approach and to reach out to a much wider international audience. Perhaps the true start of the new millennium, the year 2001, could be the start of IISSC - the International ISSC? In regard to this suggestion:

The panel will adopt the position that for businesses and individuals to truly benefit from ecommerce, technical inter-operability is neither the key issue nor a challenge. Rather, users need to know that trust in their service providers is justified, that they are subscribers to open services with no barriers to with whom they may communicate, and that they can rely upon the identity of their counter-parties throughout the trading chain.

The panelists will what ask what 'trust indicators' are really required to establish trust in an e-world. They will question the contribution that standards make and look to other means of assessing service providers, to give confidence to business and private users who.

Reference will be made to activities on-going in Europe, the US and other parts of the world to address these issues, covering work done to identify real trust indicators, various international and regional rules governing the use of electronic signatures, a scheme being

developed by European and global organisations to establish a world-wide trust infrastructure and efforts to establish standardised policies and conformance profiles.

This session will bring to a largely US audience some specific European perspectives and awareness of ongoing work. It is intended to be interactive, even provocative: members of the audience will be invited to respond and debate the issues in terms of the relevance of this work to the US business environment and exploring ways in which joint co-operation could be fostered.

Wilson, F. (1995). "Managerial control strategies within the networked organization." Information Technology & People 8(3): 57-72.

Over the last decade, a pivotal theme within management and organizational research has been the identification of new industrial methodologies and technologies which focus on the generation of greater workforce commitment and flexibility. The hope is that the new information-based technologies will allow for the tenets and practices of Taylorism and Fordism, once the basis for industrial development, to be swept away, thus developing an environment of commitment and trust. This would be exemplified by 'empowered' semi-autonomous units of production, where a highly trained and skilled workforce would exercise freedom and authority within a decentralized mode of control and coordination. To support this perspective, a number of managerial techniques such as total quality management and business processes engineering have arisen,which claim to describe the ways in which organizations may provide this autonomy, while simultaneously increasing productivity. A parallel theme has been the development of critical approaches to these events, which suggests that the use of such techniques, rather than providing radical alternatives to the precepts of scientific management, merely reinforce it. Central to this perspective is the proposition that increasingly powerful computer-based systems (CBS) coupled with quality management (QM) methodologies provide enhanced control over workforce activities and provide management with improved surveillance and disciplinary mechanisms.

This article contends that many of the new flexible forms of both production and organizational structure, which are exemplified by the concept of the decentralized 'networked organization', may be shown to dependent on both highly centralized systems and disciplinary mechanisms for their essentially integrated command, control and communications operations. Furthermore, it is suggested that, while many authors of the CBS/QM paradigm promote concepts of 'empowerment' and freedom of individual decision making, these may be seen to rest on an increasing manipulation of the individual by centralized forms of managerial surveillance and cultural control.

Wilson, P. N. and A. M. Kennedy (1999). "Trustworthiness as an economic asset." The International Food and Agribusiness Management Review 2(2): 179-193.

The evaluation of trust in economic decision making remains on the periphery of mainstream economic analysis and teaching. Yet business managers use trustworthiness in daily exchanges to create competitive advantages for their firms. An exploratory empirical test of Barney and Hansen's three levels of trust (weak, semistrong, and strong) and Lewicki and Bunker's portfolio of governance mechanisms revealed that strong-form trust exists in day-to-day business relationships along with other governance mechanisms. Identity-based transactions were more prevalent than were weak trust market exchanges in important economic transactions.

Witty, R. (2003). Five business drivers of identity and access management. Strategic Planning, Gartner Research: 8.

Wong, K. F., M. K. W. Tam, et al. (2003). An e-government software repository. e-Society 2003, Lisbon, Portugal, IADIS, International Association for Development of the Information Society.

This paper proposes a solution for a government to make a transition from conventional to Component-Based Software Development (CBSD). A set of logistics components is designed and developed to facilitate the development of government to citizen (G2C) applications, such as provision of government products and services to citizens.

Wood, D. (2003). "Foucault and panopticism revised." Surveillance & Society 1(3): 234-239.

This editorial introduces the issue in the context of the progress of the Surveillance & Society project. It discusses the theme of this issue, the importance of Michel Foucault's work for Surveillance Studies, briefly summarises the contributions of the authors, and also considers what comes next.

Yar, M. (2003). "Panoptic power and the pathologisation of vision: Critical reflections on the Foucauldian thesis." Surveillance & Society 1(3): 254-271.

This article attempts to evaluate theoretically the applicability of Foucault's Panopticon to the practices of public surveillance utilising CCTV technology. The first part maps out three "strands" in the reception of panopticism in surveillance studies, suggesting that it tends to fall into one of three broad kinds: its wholesale appropriation and application; its wholesale rejection as inadequate with respect to a supposedly "post-disciplinary" society; and its qualified acceptance subject to some empirically-dependent limitations. I then attempt in a preliminary way to supplement these three positions. In particular, I question the logical adequacy of equating visual surveillance with effective subjectification and self-discipline by drawing upon a range of philosophical and sociological perspectives. Philosophically, it is suggested that the Foucauldian
thesis may well "pathologise" the relationship between subjectivity and visibility, and thereby overlook other dimensions of our experience of vision. Sociologically, it is suggested that the precise relation between surveillance and self-discipline requires us to attend, in thnomethodological fashion, to the situated sense-making activities of subjects as the go about everyday practical activities in public settings.

Young, C. G. E. (2004). Online availability of public services: How is Europe progressing? E. C. D. I. Society.

Yuan, Y., J. Zhang, et al. (2004). "Can e-government help China meet the challenges of joining the World Trade Organization?" Electronic Government 1(1): 77-91.

China's WTO entry is expected to boost the domestic and global economy. However, achieving this goal depends on whether the government of China can succeed in adapting itself to the requirements of the WTO and synchronising itself with other members to facilitate global cooperation and economic development. The Chinese government has been working seriously to meet this challenge and the first year's experience of being a WTO member seems very successful. In this paper we analyse how an e-government development strategy would help the Chinese government take advantage of the opportunities

and overcome the difficulties of being a new member of the WTO. Key e-government initiatives are discussed in detail in three major catewgories: Government-to-Government (G2G), Government-to-Business (G2B) and Government-to-Citizens (G2C).

Zhang, J. (2002). "Will the government 'serve the people'? The development of Chinese e-government." New media & society 4(2): 163–184.

In the wake of globalization, the idea of electronic government (e-government) has become an integral part of modernization efforts undertaken by countries with a variety of political systems. This article will examine how it is being pursued in the People's Republic of China (PRC), in order to contribute to our understanding of how e-government works in a non-liberal democratic polity. The analysis will start by focusing on the issues of how the Chinese understand the concept of e-government, continue by looking at what is actually being done by the state for the purpose of establishing it, and finish with a discussion of the methods that can best be used to assess the achievements and problems that are being met.

Zureik, E. (2002). Theorizing surveillance: The case of the workplace. Surveillance as Social Sorting. D. Lyon. London, Routledge: 31-56.

Zureik, E. and K. Hindle (2004). "Governance, security and technology: The case of biometrics." Studies in Political Economy 73(Spring/Summer): 113-137.

The field of surveillance studies has blossomed during the last two decades, attracting researchers from various disciplines: law, humanities, sociology, politics, and social studies of science. Privacy concerns continue to capture the lion's share of surveillance research, with little attention being paid to the processes governing the promotion and deployment of specific surveillance technologies. The paper focuses on biometrics as one type of technology that converts images of body parts (hands, eyes, face, etc.) into unique digitized identifiers of people. It examines the arguments surrounding the use of the technology for surveillance purposes in the security-conscious post-September 11 environment, and shows the apparent linkages among governance, security, and surveillance technology.