Global Co-Operation in the New Millennium
The 9th European Conference on Information Systems
Bled, Slovenia, June 27-29, 2001

THE IMPACT OF SOCIAL ISSUES ON INTERNET POLICY MAKING

Anastasia Papazafeiropoulou, Athanasia Pouloudi

Center for Strategic Information Systems, Department of Information Systems and Computing, Brunel University
Tel: 0044 1895 203375
anastasia.papazafeiropoulou@bunel.ac.uk, nancy.pouloudi@brunel.ac.uk

ABSTRACT

The advantages that Internet as a new technology offers to business and individuals can't be fully exploited without taking under consideration a number of social issues that related with its use. Its global nature makes Internet policy making a challenging task, creating new responsibilities for policy makers world-wide. Apart from the technical (e.g. security, network availability, speed) and regulatory (e.g. legal frameworks and standardization) challenges that need to be tackled there are a number of social concerns that require special concern. It is important for policy makers to see Internet use as a social as well as a technical phenomenon. In this paper we examine how social concerns such as trust and digital democracy pertain all levels of Internet policy, posing dilemmas and influencing the construction of an effective and socially responsible strategy for the Internet.

1. INTRODUCTION

Policy implementation for Internet and electronic commerce is a complex process since policy makers, national governments in their majority, have to act in a fast changing environment where international co-operation is imperative while also dealing with special national demands (Papazafeiropoulou and Pouloudi 2000). One of the areas that policy makers have to tackle is dealing with barriers have been reported in the adoption of network technologies today. These barriers are mostly derived from factors such as lack of awareness about the opportunities offered by electronic commerce as well as lack of trust to network security. Additionally the current legislative framework, drawn before the advent of the Internet, is perceived as outdated, thus impeding the expansion of on-line transactions. As the need for appropriate policy measures that support the information society is increasing, it is important to prevent a predominantly technical, commercial or legal approach that neglects the broader social issues related to policy making.

To this end, this paper examines social issues related to Internet policy making and is structured as follows. In the next section we present the social concerns that are related to policy making in electronic commerce such as trust, privacy and digital democracy. In section 3 we discuss these concerns in the light of different policy issues arising from the use of network technologies and in section 4 we present their implications for policy making in electronic commerce. The paper concludes with the importance of a holistic approach to policy making and suggestions for further research. >

2. SOCIAL CONCERNS RELATED WITH INTERNET USE

The introduction of technologies such as the Internet in everyday life has resulted in a debate about its relative merits and disadvantages. Some of the social concerns are illustrated in the study conducted by the Stanford Institute for the Quantitative Study for Society (SIQSS 2000) concerning the social implications of Internet use. The findings of the study indicate that the Internet is an "isolating technology" that could seriously damage the social fabric of communities as users interact with other people less. The social implications of the Internet can be witnessed in organizational processes, the nature of work, learning and education, innovation and competition, electronic democracy, privacy and surveillance (Dutton, 1996).

The most commonly discussed social concern in the cyberspace is trust. Trust is a key issue and its existence among the business community and the end-consumers will increase the willingness of trading partners to expand their electronic transactions (e.g. (Hart and Saunders 1997; Miles and Snow 1992; Ratnasingham 1998; Wilson 1997). The low level of trust to the Internet can be attributed partly to the lack of face-to-face interaction between trading partners in conjunction with the general uncertainty of users in taking advantage of network technologies (Ratnasingham 1998).

Information and communication technologies offer opportunities for governments and citizens to be brought into closer dialogue as well as for enhancing opportunity for political organization and debate (Raab, *et al.*, 1996). However, the extent to which the information superhighway can fully enable citizens to participate in this emerging 'digital democracy', has been heavily debated. First, at a conceptual level, our understanding of democracy is "as bounded in time as it is rooted in space" (Nguyen & Alexander, 1996, p. 120), which means that the term digital democracy is inherently problematic in 'cyberspace'. Importantly, there is a concern that if citizens are not able to have access to on-line services, because they do not have the means or the knowledge to do so, existing patterns of inequalities will be reinforced. The digital democracy is threatened by "information aristocracy" (Carter 1997). In particular, there is evidence of a gender and race gap in the use of Internet as well as differences for users with different levels of income and education (Hoffman and Novak 1999; Kouzmin *et al*, 1999).

At a global level, the Internet penetration in developing countries is also an outstanding issue related to the "haves" and "have-nots" in cyberspace, e.g. (Bhatnagar 1997; Blanning et al. 1997; Clark and Lai 1998; Kim and Hong 1997). Easy global information access, however, is also problematic as it has been described as threatening both cultural identity and the regulatory sovereignty of the state, especially when used in less powerful economies (Shields, 1996).

Finally, as privacy protection is a major concern in electronic commerce there is a concern on whether 'cyberspace' can promote democracy while protecting privacy. The free information flow of democracy and the users' need to control the flow of personal data can be seen as zero-sum alternatives that may (or may not) be balanced (Raab 1997). This generates several policy dilemmas, which are reviewed in the following sections.

3. EMERGENT INTERNET POLICY ISSUES

The fast expansion of the Internet in the last decade was exceptional, forcing policy makers to speed up their efforts for its governance and regulation. In this section we describe policy issues that need to be addressed in order to facilitate the development of a safe and well-defined environment for the users, addressing the social concerns outlined in the previous section. These policy issues are presented following the six levels of Internet policy architecture including infrastructure, governance, security, privacy, content and commerce. These have been defined by the Global Internet Project (GIP), a group of senior executives from leading companies around the world (Patrick 1999). The second part of the section presents the dilemmas in addressing policy issues, leading on to a discussion of the implications for policy makers in the remainder of the paper.

3.1. Policy Issues at Six Levels of Internet Policy

Infrastructure. The infrastructure level aims at addressing "the challenge of meeting the demand for reliable and scaleable access to the Internet" (Patrick 1999, p. 106). The speed, the quality, the reliability and the cost of the networks used for on-line transactions, are very important factors that can either boost or obstruct the evolution of electronic commerce. One of the top priorities of governments is the support of the telecommunication industry so that it can offer better quality services in terms of speed, reliability, continuous access and interconnectivity between subnetworks (Patrick 1999). The American government, for example, aims at the provision of on-line services to the majority of the American households not only through desktop computers connecting to the Internet, but also through devices such as television, cellular phones and portable digital assistants (US Department of Commerce 1998). The liberalization of the telecommunication market is a relevant directive of the European Union (EC 1997) and OECD (OECD 1997b) to their member states. It demonstrates the intention of international policy making organizations to reduce the cost and improve the robustness of the telecommunication infrastructure world-wide.

Global coverage is a major concern for policy makers today (Hudson 1999). Within a national context, the quality of the telecommunication infrastructure in rural areas is particularly significant, when the accessibility to alternative means of obtaining information is very limited. Overall, as the role of the nation state declines in providing access to telecommunications networks, it may be up to independent bodies to support citizens gaining access to Internet-delivered services (Keenan & Trotter, 1999).

Governance. The Internet is characterized by its ability to expand without central governance. It is the intention of the policy makers at an international level to support industry leadership and self-regulation for electronic commerce (The White House 1999; EC 1997; OECD 1997b). Specifically, there is a tendency to minimize government involvement and avoid unnecessary restrictions on the Internet.

However, as Internet use becomes mature its international nature creates the need for global governance in certain areas. For example, several legal cases have been reported that involved web sites owners and consumers or other companies. The conflict usually derives from the lack of certainty about where a web company is physically located and thus under which country's legal system the company works (Aalberts and Townsend 1998).

Taxation is a specific concern for companies that intent to invest in new technologies and for governments that want to control electronic commerce similarly to traditional commerce. There is a wide range of proposals concerning the administration of taxes in electronic commerce (Johnston 1999; Owens 1999). At one extreme there is the idea of absolute 'tax free' electronic commerce that has already been implemented for transactions taking place among US states, until February 1998 when the US public administration reaffirmed its commitment to making cyberspace a free-trade zone (Negroponte 1999). At the other end there are proposals for introduction of special new taxes for electronic commerce. OECD (OECD 1997a), proposes an intermediate solution, directing its members to apply existing tax principles in electronic transactions.

Overall, the governance level presents a challenge for national policy makers as they realize on the one hand that it is difficult, if not impossible, to control electronic transactions. Also, it is debatable what is within a specific jurisdiction or how 'Netlaws' will be enforced or who will pay for enforcement (Shim, *et al*., 2000). On the other hand, policy makers are also keen to promote electronic transactions with minimal intervention, as they want to attract investors that will contribute to economic growth.

Security. Network security and especially web security is one of the most sensitive issues identified in the literature (e.g., (Crocker 1996; Kosiur 1997; Liddy 1996). A recent survey of Australian firms (Dinnie, 1999), "among the world's earliest adopters" of electronic commerce, reports that network security is a continuing concern and companies are more concerned about external threats. The survey reports that "sixteen per cent of firms have suffered, or believe they may have suffered, at least one break-in via the Internet" (p. 112). Despite their perceptions of external threats, however, thirty per cent of businesses admitted that their organization had no formal information security policy procedures. More generally, the

anxiety about security is expected to increase in coming years as web-based applications are increasingly used for financial transactions. As the number of computers, networks, data and information multiply every day, the need for better security practices that protect information systems from malicious attacks and at the same time preserve the civil liberties, will increase in the future (Hurley 1999).

Cryptography is put forward as a powerful technological solution to network fraud. At an international level it can be applied with the collaboration of governments, business community and trusted third parties (Denning 1996). The required use of public and privet keys in cryptography methods, raises several public policy issues surrounding the encryption of data and who should hold the keys that unlock the encrypted information (Patrick 1999; Pouloudi 1997). Policy makers can play an important role in the implementation of a security policy, acting as trusted third parties or defining the legal framework for such organizations (Froomkin 1996). There are multiple models concerning the role of governments in security policy. At one extreme, public authorities may have ultimate access to information and at the other, they may leave the responsibility for security of the data to the information owner (Patrick 1999). What seems to be urgently required today is more education and awareness of security of information systems and good security practices for companies and individuals (Hurley 1999).

Privacy. Computer technologies like the Internet facilitate the exchange of personal information that can be collected, aggregated and sold across the world. As people and companies can easily gain from the personal information that becomes accessible on information networks, e.g., through direct marketing (Wang, *et al.*, 1998), several issues are at stake. The most important concern is whether information is collected, aggregated or sold with the individual's explicit concern. There are several private organizations (Better Business Bureau on Line (BBBOnLine), Worldwide Web Consortium (W3C), TRUSTe) that try to address the issue by giving a privacy 'seal' to web sites that are fulfilling some set criteria of privacy protection. These include the responsibility to make visitors to web sites aware of what data is collected and giving them choice about making this data available to third parties.

Privacy is particularly important for the protection of sensitive personal data such as medical records, credit records, government data and personal data about children. The US government has taken a regulatory approach to protect such information leaving self-regulation by the private sector in any other case. The aim is to enable Internet users to choose for themselves what level of privacy protection they want (Nelson 1999). In Europe, in contrast, data protection is much tighter and has been articulated at a pan-European level (Allaert & Barber, 1998). In the United States, the EU directive (EC 1992) has been perceived as being overprotecting for European companies, raising barriers to the free exchange of electronic data between Europe and other countries (Swire and Litan 1998). Indeed, the European directive on data protection challenged electronic transactions and data exchanges internationally, as it banned the export of personal data from the EU to those countries without strict federal data protection laws. This included the US, and resulted in severe trade disputes at an international level, which has been resolved recently with the Safe Harbor Privacy Arrangement. This is a mechanism, which, through an exchange of documents, enables the EU to certify that participating U.S. companies meet the EU requirements for adequate privacy protection. Participation in the safe harbor is voluntarily. Privacy advocates, however, argue that privacy is a profound and fundamental concept, hence "it merits extra-ordinary measures of protection and overt support" (Introna, 1997, p. 259).

Privacy therefore clearly raises social concerns, particularly in relation to the rights of employers to access or monitor personal information of their employees (ranging from email messages to medical records), often without their explicit consent or even their knowledge. While the European directive sets a general framework for data protection within Europe, the difficulties of updating databases and business processes and the challenges to comply at a technical level when using some contemporary information technologies (Lycett & Pouloudi, 1999) signify that privacy protection remains a challenge for policy makers.

Content. As electronic commerce is an international phenomenon it is impossible for policy makers to control the content of the information transferred on-line. While the exposure to all this information can be beneficial, for example expanding people's learning horizons (Forcheri, *et al.*, 2000), governments and citizens are concerned about the publication of offensive material (Nelson 1999). As the complaints from

parents and educators about the influence of the Internet on children become more frequent, there are several civil liberties organizations devoted to protect users form exposure to inappropriate on-line material. Such groups include the Electronic Frontier Foundation (EFF), which supports legal and legislative action to protect the civil liberties of on-line users and the Computer Professionals for Social Responsibility (CPSR), which aims to protect privacy and civil liberties. The World Wide Web Consortium (W3C) has developed a technical platform that allows user-defined, customized access to the Internet (Patrick, 1999; www.w3.organisation/PICS) and has enabled the creation of rating services and filtering software, for example for use by concerned parents. While the need for filtering of some information is generally considered as appropriate, there are also attempts at censorship. For example certain Asian countries place restrictions in the use of the Internet. The use of censorship on the information highway is debatable, both in terms of its technological feasibility but also in terms of its moral foundation (Ebbs & Rheingold, 1997).

Other content related issues in electronic commerce are the protection of copyright and intellectual property rights. The essence of copyright is to prevent the unauthorized copying, but works stored in a digital format can easily be copied or altered, while they can also be transmitted speedily through electronic networks (Brett 1999). The practical problems that owners of digital data face are a very important issue for governments trying to apply or extend existing copyright laws to digital means. As with other policy issues, intellectual property involves multiple stakeholders with different interests (Radcliffe, 1999), which makes it difficult to resolve at a global level.

Commerce. Electronic commerce is at the top of the policy architecture pyramid of the Global Internet Project, as it is perceived to be a critical factor driving the growth of the Internet. Although electronic commerce has revolutionized they way of conducting business, it is still a business activity that has to conform to certain rules and work under specific standards (Negroponte 1999). The European Union was the first official body that considered a supranational policy on electronic commerce, in its effort to advance the integration process and to create a single market (Mc Gowan 1998). However, there are several organizations working at a supranational level trying to enable global seamless communication such as the International Organization for Standardization (ISO), and the World Trade Organization (WTO). This is because standardization is recognized as an important issue in electronic commerce, since the establishment of EDI applications (e.g., (Chatfield and Bjorn-Andersen 1998; Faltch 1998; Sokol 1995; Tan 1998).

The discussion in the previous five levels of the policy architecture demonstrates that social issues are relevant at all levels, and indeed underpin the development and use of the Internet. The problem is that most of these issues cannot be easily resolved as they bring about conflicts amongst stakeholder groups and policy dilemmas. These are discussed in detail below.

3.2. Dilemmas in Addressing Policy Issues

Previous research has argued that the policy objective of promoting deregulation and competition is in conflict with other policy priorities, in particular the desire to provide open networks and open access and the aspiration to provide universal service to citizens (Graham, 1995). As Internet expands, the dilemmas for the stakeholders of the information society increase. The review of policy issues at different levels in the previous section has revealed some of these dilemmas:

- Where should priority be given: to the protection of personal data or to competitiveness (to the extent that the free exchange of information and personal data supports electronic transactions and business practices)?
- Is governance about protection or restriction? At an individual level, is censorship desirable? What is more important, data and intellectual property protection or the free exchange of ideas and data? At a business level, is taxation desirable? More generally, should self-regulation prevail in various industry sectors or is regulation still the responsibility of national governments?
- What is more important, data and intellectual property protection or the free exchange of ideas and data?

- Does the need for more technical education justify the specialisation of the younger generation in areas related to the Internet development at the expense of social science education in areas such as history and sociology?

These dilemmas relate to the appropriate use of regulation, although in some cases policy makers may have little choice as only some options are realistic (e.g., the Internet is used even though the legal context is unstable). Thus, one important observation is that some dilemmas may no longer be a matter of choice, particularly for less powerful stakeholders, such as individuals, or governments of developing countries. A further observation is that in many cases these dilemmas imply a conflict between the commercial and social interests of various stakeholder groups. However, it is very difficult to draw some general conclusions about when either interest is at stake. Research in management (e.g., Pettigrew, 1985) and information systems (e.g., Walsham, 1993) as well as in law studies (e.g., as evident in the importance of case law) has stressed the importance of context. However, in 'cyberspace' the context, whether temporal or spatial, is elusive, making policy making for electronic commerce more challenging.

4. IMPLICATIONS FOR POLICY MAKERS

The challenge that policy makers face today in order to implement an efficient Internet policy while addressing the dilemmas outlined above is twofold. Firstly, they need to provide the business community with a robust technical infrastructure and an efficient legislation framework. Secondly, they need to accommodate the social concerns rising from the use of network technologies, in order to create a 'digital literate' society that will fully exploit the technology at hand while preserving their social interests and cultural identities.

As discussed earlier in the paper, other policy intermediaries that become increasingly involved in policy issues in the information society include independent private organizations as well as civil liberties and professional groups who wish to promote the interest of a particular group or the net-citizens at large. Schools and Universities also face pressures to support the 'workforce of the future' and try to promote the use of information and communication technologies, thus contributing to knowledge building and deployment strategies. Finally, the Internet empowers individuals to draw their own policies at a micro-level, e.g., choosing, as parents, which Internet sites they allow their children to access, deciding whether to make their personal information available and so on. While the Internet enables people as citizens and consumers to take action (e.g., Badaracco & Useem, 1997), people are not necessarily aware of the opportunities and risks of cyberspace or the may not have the power and access to make a difference. Policy makers, whether local or national, government or private, need to recognize the prevalence and importance of social issues and encourage the debate for appropriate policy making amongst stakeholders.

5. CONCLUSIONS

Policy makers have recognized the viability of Internet and the opportunities it offers for business and citizens. While several ethical and social issues arise from the use of the new technologies there is a general consensus that the benefits are substantial and justify the investment in network technologies. There are several efforts in this direction by policy makers at a national and international level. The paper has argued that technology alone is not sufficient for the successful implementation of complex electronic commerce strategies but the examination of social and political issues is crucial for a holistic approach on the subject. Indeed there are several dilemmas related to policy issues, making the role of the policy makers critical. We considered a general framework for policy making that could be used at a national or international level as a starting point for considering social issues in the context of electronic commerce strategies.

Further research in the area may include the investigation of electronic commerce policies implemented in different national settings and social environments since in practice different countries have different priorities. The case of developing countries would be of particular interest as technical infrastructure and stakeholder awareness and involvement can be substantially different. Research also needs to be continued in

specific areas that are affected by the extensive use of the Internet. Because of their social importance, of particular interest are the areas of health and education where issues of Internet use and electronic commerce become increasingly relevant (e.g., through telehealth or distance learning applications). A study of alternative national policies in these areas can lead to an informative debate about the underlying assumptions concerning the duties and social responsibility of policy makers towards different stakeholder groups.

Acknowledgements

The authors gratefully acknowledge the financial support of EPSRC grant GR/N03242

REFERENCES

Aalberts, R., and Townsend, A. (1998). The threat of long-arm jurisdiction to electronic commerce. *Communications of the ACM*, 41(12), 15-20.

Allaert, F.-A., & Barber, B. (1998). Some systems implications of EU data protection directive. *European Journal of Information Systems*, 7 (1), 1-4.

Badaracco, J. L., Jr, & Useem, J. V. (1997). The Internet, Intel and the Vigilante Stakeholder. *Business Ethics: A European Review*, 6 (1), 18-29.

Blanning, R., Bui, T., and Tan, M. (1997). National information infrastructure in Pacific Asia. *Decision Support Systems*, 21, 215-227.

Brett, H. (1999). Copyright in a digital age. Masters of the wired world, A. Leer, ed., Financial Times Pitman Publishing, London, 162-171.

Carter, D. (1997). 'Digital democracy' or 'information aristocracy' Economic regeneration and the information economy. The Governance of Cyberspace, B. Loader, ed., Routledge, London, 136-152.

Chatfield, A., and Bjorn-Andersen, N. (1998). Reengineering with EDI. A Trojan horse in circumventing non-tariff barriers to trade. EDI and Data Networking in the Public Sector, K. V. Andersen, ed., Kluwer Academic publishers, 155-172.

Clark, J., and Lai, V. (1998). Internet comes to Morocco. *Communications of the ACM*, 41(2), 21-23.

Dinnie, G. (1999). The Second Annual Global Information Security Survey. *Information Management & Computer Security*, 7 (3), 112-120.

Dutton, W. H. (Ed.). (1996). *Information and Communication Technologies: Visions and Realities*. Oxford: Oxford University Press.

Ebbs, G., & Rheingold, H. (1997). Censorship on the information highway. *Internet Research: Electronic Networking Applications and Policy*, 7 (1), 59-60.

EC. (1995). Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, L281(23 Nov 1995), 31.

EC. (1997). A European Initiative in Electronic Commerce' (COM (97) 157 final), EC (European Commission), Brussels.

Faltch, M. (1998). EDI in the Public Sector: Building on lessons from the private sector. EDI and Data Networking in the Public Sector, K. V. Andersen, ed., Kluwer Academic publishers.

Forcheri, P., Molfino, M. T., & Quarati, A. (2000). ICT driven individual learning: new opportunities and perspectives. *Educational Technology & Society*, 3 (1), 51-61.

Graham, A. (1995). Public policy and the information superhighway: the scope for strategic intervention, co-ordination and top-slicing. In R. Collins & J. Purnell (Eds.), *Managing the information society* (pp. 30-44). London: Institute for public policy research

Froomkin, A. (1996). The essential role of Trusted Third Parties in Electronic Commerce. Readings in Electronic Commerce, R. Kalakota and A. Whinston, eds., Addison-Wesley.

Hart, P., and Saunders, C. (1997). Power and trust critical factors in the adoption and use of electronic data interchange. *Organization Science*, 8(1), 23-41.

Hoffman, D., and Novak, T. The evolution of the digital divide: Examining the relationship of race to Internet access and usage over time. *Understanding the Digital Economy: Data, Tools and Research*, Washington, USA.

Hudson, H. Access to the digital economy: issues in rural and developing regions. *Understanding the digital economy*, Washington, USA.

Hurley, D. (1999). Security and privacy laws. The showstoppers of the Global Information Society. Masters of the wired world, A. Leer, ed., Financial Times Pitman Publishing, London, 247-260.

Introna, L. D. (1997). Privacy and the computer: why we need privacy in the information society. *Metaphilosophy*, 28 (3), 259-275.

Keenan, T. P., & Trotter, D. M. (1999). The changing role of community networks in providing citizen access to the Internet. *Internet Research: Electronic Networking Applications and Policy*, 9 (2), 100-108.

Kim, E., and Hong, P. (1997). The government's role in diffusion of EC in Korea. *Electronic Markets*, 7(2), 6-8.

Kouzmin, A., Korac-Kakabadse, N., & Korac-Kakabadse, A. (1999). Globalization and information technology: vanishing social contracts, the "pink collar" workforce and public policy challenges. *Women in Management Review*, 14 (6), 230-251.

Lycett, M.G. & Pouloudi, A. (1999) Issues of data protection in contemporary development environments. ETHICOMP99 - The Fifth International Conference on the Social and Ethical Impacts of Information and Communication Technologies. 6-8 October 1999. LUISS Guido Carli University, Rome, Italy.

Mc Gowan, L. (1998). Protecting competition in a global market: the pursuit of an international competition policy. *European Business Review*, 98(6), 382-339.

Miles, R., and Snow, C. (1992). Causes of failure in network organizations. *California Management Review*, summer, 53-72.

Negroponte, N. (1999). Being digital in the wired world. Masters of the wired world, A. Leer, ed., Financial Times Pitman Publishing, London, 386-394.

Nelson, M. (1999). Politics and policy-making in the electronic marketplace. Masters of the Wired world, A. Leer, ed., Financial Times Pitman Publishing, London, 261-269.

Nguyen, D. T., & Alexander, J. (1996). The coming of cyberspacetime and the end of the polity. In R. Shields (Eds.), *Cultures of Internet: virtual spaces, real histories, living bodies* (pp. 99-124). London: Sage.

OECD. (1997a). The Communication Revolution and Global Commerce: Implications for tax policy and administration, OECD (Organization for Economic Co-operation and Development).

OECD. (1997b). Global Information infrastructure-global information society (GII-GIS), Policy requirements, OECD (Organization for Economic Co-operation and Development).

Owens, J. (1999). Electronic commerce: taxing times. Masters of the wired world, A. Leer, ed., Financial Times Pitman Publishing, London, 286-295.

Papazafeiropoulou, A., and Pouloudi, A. (2000). The Government's Role in Improving Electronic Commerce Adoption. In H.R. Hansen et al., (Eds.) Proceedings of the European Conference on Information Systems 2000 vol. 1, (pp. 709-716). July 3-5. Vienna, Austria.

Patrick, J. (1999). The opportunity and the challenge to sustain rapid Internet growth. Masters of the wired world, A. Leer, ed., Financial Times Pitman Publishing, London, 105-112.

Pettigrew, A. M. (1985). Contextualist research and the study of organisational change processes. In E. Mumford, R. Hirschheim, G. Fitzgerald, & T. Wood-Harper (Eds.), *Research Methods in Information Systems* (pp. 53-78). Amsterdam: Elsevier Science Publishers, North-Holland.

Raab, C. (1997). Privacy, democracy, information. The Governance of cyberspace, B. Loader, ed., Routledge, London, 155-174.

Raab, C., Bellamy, C., Taylor, J., Dutton, W. H., & Peltu, M. (1996). The Information Polity: Electronic Democracy, Privacy, and Surveillance. In W. H. Dutton (Eds.), *Information and Communication Technologies* (pp. 283-299). Oxford: Oxford University Press.

Radcliffe, M. (1999). Intellectual property and the global information infrastructure. Masters of the wired world, A. Leer, ed., Financial Times Pitman Publishing, London, 105-112.

Ratnasingham, P. (1998). The importance of trust in electronic commerce. *Internet research: Electronic Networking Applications and Policy*, 8(4), 313-321.

Shields, R. (Ed.). (1996). *Cultures of Internet: virtual spaces, real histories, living bodies*. London: Sage.

Shim, J. P., Simkin, M. G., & Bartlett, G. W. (2000). NetLaw. *Communications of the Association for Information Systems*, 4 (4).

SIQSS. (2000). Internet and society, Stanford Institute for the Quantitative Study for Society.

Sokol, P. (1995). *From EDI to Electronic Commerce*, McGraw-Hill.

Swire, P. P., and Litan, R. E. (1998). *None of your business. World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press, Washington, D.C.

The White House. (1999). Facilitating the growth of electronic commerce, The White House, Washington.

US Department of Commerce. (1998). The Emerging Digital Economy, US Department of Commerce, Washington.

Walsham, G. (1993). *Interpreting Information Systems in Organizations*. Chichester: Wiley.

Walsham, G. (1999). GIS for district-level administration in India: problems and opportunities. *MIS Quarterly*, 23 (1), 39-66.

Wang, H., Lee, M. K. O., & Wang, C. (1998). Consumer privacy concerns about internet marketing. *Communications of the ACM*, 41 (3), 63-70.

Wilson, S. (1997). Certificates and trust in electronic commerce. *Information Management & Computer Security*, 5(5), 175-181.