
# E-VOTING: INSIGHTS FROM COMPARATIVE PUBLIC POLICY

## eDC e-Paper Series

## 2003/01

By

**Fernando Mendez**

**ABSTRACT**

In this paper I take a broad look at a number of policy areas which have been especially impacted by the Internet and refer to this as the 'e-policy' domain. I then attempt to probe whether any insights from the so-called e-policy domain are relevant to the case of e-voting. In looking at some of the areas that have been most directly affected by the Internet I identify a tension between openness and closedness and draw attention to the important role of perceptions, especially those associated with technological risk. The conclusion drawn is that if these insights are relevant to the case of e-voting, then it is likely that future e-voting arrangements will exhibit significant cross-national variation.

**E-Democracy Centre**
Université de Genève
Faculté de Droit
40, bd du Pont-D'Arve
CH-1211 Genève 4
Switzerland

edc@droit.unige.ch

I begin by taking a broad look at some of the policy areas that have been most impacted by the Internet and refer to this as the ‘e-policy’ domain. A disclaimer should be issued at this stage with regard to the e-policy domain: It does not represent a coherent whole but rather a serries of overlapping and myriad policy areas which have to some degree been affected by the explosion of the Internet. The overall aim, in any case, is not to try and define this admittedly amorphous policy domain, but rather to probe whether we can derive any insights from the e-policy context which may shed some light on pertinent issues related to e-voting. In looking at some of the areas that have been most directly affected by the internet we find that a lot of the problems that the internet raises are not so much new problems as old problems in new guises. Could this also be the case for e-voting?

The core regulatory dilemmas that afflict the so-called e-policy domain could be succinctly illustrated by viewing the Internet through two conflicting lenses. On the one hand engineers view the Internet as an astonishingly elegant and seamless global information network that transcends national borders. This is indeed the case. Lawmakers and politicians, on the other hand, are confronted with a jurisdictional quandary with major regulatory fault lines emerging in areas such as taxation, applicable law, copyright and content, to name but a few. In the context of the e-policy domain resolving these conflicts will require a delicate balancing between competing interests and, in many cases, authoritative political resolution. The internet technologies may favour speed and decentralisation politics, however, can be a slow and consensus seeking business characterised by an incredible sensitivity to particular issues. This dialectical tension between ‘architecture’ and ‘politics’ is at the core of the e-policy dilemma –we would expect the same to apply to the case of e-voting.

Intriguingly, when one applies a similar optic to e-voting a remarkable inversion of positions is evident. While politicians [1]may trumpet, at least at the rhetorical level, the potential of e-voting for connecting with the electorate it has largely been the epistemic community formed by technologists and engineers that has expressed the gravest doubts as to the viability of internet voting. We will return to this issue, which raises fundamental questions as to perceptions of risk among this very influential community, in greater detail below.

There is thus at the heart of the internet public policy debate a tension between the possibilities offered by the technical architecture and the menu of political options available to policymakers[2]. The two are, of course, interacting. This view differs, quite markedly, from the earlier literature concerning the Internet and its transformative potential which tended adopted a uni-causal lens whereby technology would eventually structure and determine political choices. At the risk of grossly simplifying some of the earlier literature two views were offered. The rosier vision envisaged the emergence of an E-topia. As we moved away from the 'atom' society to the 'bit' (i.e. digital society) the structure of society, the economy and current forms of political organization would be transformed[3]. An alternative but dystopian future was offered by others for whom the internet threatened to unleash unstoppable technical forces, such as cyber terrorism, which would mark the demise of state power[4]. While the respective prognoses may have differed they both shared a similar

[1] See for instance the chairman of the British Cabinet's e-democracy committee, Robin Cook, interview with The Guardian 'Cook plans to make UK first to vote on internet' by Jackie Ashley, 7 January 2002 available at: http://www.guardian.co.uk/internetnews/story/0,7369,628776,00.html

[2] One of the most sophisticated analysis of this interaction is offered by Lessig's seminal work, see in particular Lessig 1999. Code and other laws of cyberspace . New York: Basic Books;.

[3] This view is offered by Negroponte, Nicholas. Being Digital. New York: Knopf; 1995.

[4] See for instance Angell, Ian 'The Real Politik of the Information Age' Information Strategy, January 1998

techno-deterministic diagnosis. Over the past years somewhat of a reversal has been evident as some of the earlier hyperbolic statements have given way to a more sober assessment. In this vein it is not surprising that two eminent international relations scholars, Robert Keohane and Joseph Nye, would be among those to challenge, at the height of the internet and e-commerce boom, the wisdom of such earlier prognostications especially those that concerned the demise of the nation-state[5]. They ascribed a primacy to the inherent adaptability of the nation-state, which could among other things seek greater international co-ordination in the context of a digitally injected version of globalization. This is indeed happening with greater international co-ordination visible –usually via international treaties - in such diverse areas as protection of intellectual property rights, data protection regimes and even in the case of cybercrime. The problem with some of the earlier cyber fantasies is that they parted from the misguided assumption that the virtual world was somehow independent from the real world. It is not and this may have profound implications, especially for the case of e-voting.

Recent scholarship on the internet and its public policy implications has revealed that many of the fundamental policy issues that are raised are not so much new problems as old ones that appear in new guises[6]. A few examples will suffice to illustrate the argument, which may be relevant to the case of e-voting. In the domain of data protection there has long been a tradition of regulation in the privacy sphere. The first wave of reform in most western legal systems emerged in the 1970s and 1980s. This

[5] Keohane, Robert and Nye Joseph S. Power and Interdependence in the Information Age. Foreign Affairs. 1998; Volume 77(5).

[6] See for instance Cohen, Stephen and Delong Bradford and Zysman John. Tools for Thought: What is new about the 'E-conomy'. Berkeley Roundtable on the International Economy. 2000(Working Papers 138). Also see Zysman, John and Weber Steven. Governance and Politics of the Internet Economy-Historical Transformation or Ordinary Politics with a New Vocabulary? Berkeley Roundtable on the International Economy . 2000 May (Working Paper 141).

legislation was a reaction to the new challenges to privacy caused by expanded possibilities for collecting, storing and transmitting data by new technologies. Data protection laws were enacted and have been constantly revised updated and aimed at protecting the citizens' right to privacy. Seen from this light the privacy question is not a new one, although the Internet does accentuates an old policy problem that has pitted civil liberties groups against government for decades. Nonetheless there have been shifts that alter the fundamental nature of the problem. The old policy problem concerned steps to prevent government abuses but in the recent years the private enterprise has increasingly replaced national government as the largest potential threat to personal data abuse. A difficult balance between the privacy interests of the data subjects and the freedom of the holders of personal data has to be struck. In the case of e-voting serious privacy questions are raised, especially where private parties are involved in the electoral process.

Another policy area that has been significantly impacted by the internet is intellectual property rights. Although intellectual property issues have been a significant subject of law for many years (the origins of current international efforts to address intellectual property protection dating back to the Paris and Berne Convention's of the late 19$^{th}$ century) the Internet today plays the dominant role in the illegal distribution of software and other protected products. Users are able to use all kinds of online communication facilities, e-mail or bulletin boards, to facilitate the downloading of copyright protected material. At the heart of the challenge is the massive discrepancy between the costs of producing a work, program etc and the negligible cost of reproduction. This explains the vigorous demand on the part of rightholders for protective regimes, with two of the most salient copyright products, from a cyber

perspective, being software and music. Another example that illustrates the notion of an old problem in a new guise is in relation to dealing with illegal and harmful content on the internet. There has long been a tradition of regulating the content of new media with legislators, by and large, succeeding in imposing some forms of restrictions on content that they perceive to be harmful. At certain historical junctures, which usually coincide with the emergence of a new media form, issues related to censorship and content regulation can literally explode into the public domain and generate moral panic. In this respect the heated debate concerning pornography and other 'harmful' material freely available on the Internet, follows a classic pattern of moral panic throughout the ages. A succession of new media, the novel, the cinema, television, video, computer games have all generated recurrent waves of public anxiety, especially during the early stages of their introduction.

The point of this policy detour is to underline the argument that e-voting is likely to raise age old issues in new guises. Transformative e-voting arrangements, such as new platforms facilitating an unprecedented degree of deliberation or participation possibilities, raise issues that hark back to Athenian democracy. Who would be the potential winners or losers from such new voting arrangements and what are the normative implications of promoting different models of democracy, e.g. participatory versus more deliberative models. Some potential insights to these questions can certainly be gleaned from the e-policy domain. Just as lessons from the e-commerce domain have taught us that the internet cannot alter the fundamental economic laws of demand and supply one ought not to expect e-voting to provide a digital panacea[7] for

[7] For a skeptical account see Norris, P (2002) 'E-voting as the Magic Ballot? The impact of internet voting on turnout in European Parliamentary elections' Paper presented for the conference on *E-voting and the European Parliamentary elections*, held at the Robert Schuman Centre for Advanced Studies in Florence, May 10 and 11, 2002.

the purported crisis that is commonly said to afflict modern democracies. Notwithstanding these disclaimers it is possible that e-voting, assuming it goes further than merely improving voting convenience, could provide for some real innovations.

Thus far we have emphasized the rather intuitive notion that e-voting, however novel, will tend to raise old issues as has been the case in other e-policy areas. Let us now try to unpick this notion of the e-policy domain somewhat further. That the Internet poses a challenge for policymakers is now old news and is well documented by a multitude of studies. What is revealing, however, is the nature of this challenge. On the one the Internet is seen as a vital tool for enhancing competitiveness. This calls for 'enabling' type policy initiatives to establish favorable regulatory environments that are conducive to innovation and commerce. Examples include e-commerce initiatives and, more pertinent for the case of e-voting, the so-called e-government strategies that are being pursued by most advanced industrial nations. On the other hand the Internet also poses a series of negative challenges. Whether it is in the form of facilitating cyber attacks on critical infrastructures or disseminating child pornography the Internet is seen as a threat to certain aspects of the established order. These include the aforementioned examples of data protection, copyright rules and dealing with the dissemination of illegal and harmful content. Thus, when surveying the e-policy terrain one can distinguish between proactive policies that aim to channel the positive and enabling aspects associated with the Internet and another set of policies that attempt to address the negative fallout. Clearly the case of e-voting falls within the more enabling and proactive strategies. But this would be a very partial account –we have to dig deeper in order to gain a more complete understanding of the issues at

stake. Let us take e-government as an example of the tension that is at the core of the e-policy dilemma. To aid us in the conceptualization we could imagine a continuum ranging from a very open e-government model at one end of the spectrum to a more closed model at the other end. At the open end of the continuum citizens may be able to interact with government in a way that goes further than say, merely filling online tax receipts, but offers real possibilities for greater democratic deliberation and participation in decision-making processes. At the closed end of the continuum e-government consists of a leaner and more efficient internal public administration model with only limited scope for democratic interaction between government and citizen. Let us refer to this, for want of a better label at this stage, as the tension between *openness* and *closedness*. One of our core assumptions is that this problematique, between the open and the closed, permeates most of the policy debates concerning the Internet. Could this be the same for e-voting? The tension is manifest whether one focuses on copyright (fair use versus strong copyright rules); online privacy (voluntary codes of conduct for data controllers versus strong data protection regulatory regimes); software (open source code versus proprietary software); computer security (; taxation (tax moratorium on internet transactions versus taxation); illegal and harmful content (user empowering filtering technologies versus top-down censorship); e-government (openness in terms of encouraging citizen to government communication and more closed versions to improve the internal efficiency of public administration). Could e-voting arrangements be characterized by a similar tension between open models and others that are more closed? One could distinguish between different models of e-voting from the more closed systems where voting takes place in controlled environments such as public voting kiosks to more open systems that allow for remote voting from the home.

The internet in this respect raises some thorny issues as to what constitutes an appropriate mix between the open and closed. In some cases old policy bargains will be challenged, as has occurred with regard to online taxation and copyright laws. Sometimes the market will decide the appropriate mix between openess and closedness as in the case of computer software. In others it will becomes a public policy question that requires authoritative political resolution from lawmakers. In the case of e-voting a political decision will be required, firstly to decide whether or not to offer the possibility and secondly to decide the appropriate mix between the open and the closed –e.g. between full-scale internet voting from the home and a more limited version, say at controlled kiosks. The key point is that the appropriate mix is not necessarily a neutral, or for that matter even a technological question. It will depend, as it does in other e-policy areas, on many factors such as political cultures, policy styles and crucially –given the serious security concerns that are raised- on perceptions of risk. classic examples from the e-policy domain concerns the transatlantic divergence on the issue of online privacy where the EU and the US have opted for different regulatory regimes for the protection of personal data. Are there any lessons to be drawn for e-voting? The most obvious, if the e-policy context is anything to go by, would be to expect cross-national variations in potential e-voting arrangements[8]. This would be the result of not only differences in policy styles, traditions of democracy and constitutional factors but also, crucially, as a result of differences between perceptions of risk. The latter could profoundly influence the type of e-voting arrangement that is sought and subsequently implemented. While the

[8] Variations could exist with states as well, in the local elections of May 2nd in Britain no less than 31 separate trials of innovative voting methods –mostly of an electronic nature- are taking place among the most innovative are arrangements to allow voting via mobile phones.

constitutional factors have been considered elsewhere [9] the role of risk perception has –to my knowledge- not yet been adequately studied.

By focusing on the notion of risk perception, or more specifically perceptions of technological risk, it is hoped that some further insights may be gained for the case of e-voting. In spite of the fact that the first binding political elections that allowed voters to cast their ballots via internet –the 2000 Arizona Democratic Presidential Primary- took place in the US most studies and reports conducted in the US have been lukewarm at best. Moreover, one of the most influential of these, a report from the US National Science Foundation [10], is patently skeptical about the idea. The risks –according to this particular community of researchers- are far too great at this early stage and the technology is still too uncertain. But will task forces from other nations necessarily reach the same conclusions? Just because an eminent US institution has given internet voting the 'thumbs down' does not mean that other task forces will reach the same conclusions –although to date this has arguably been the case. To shed some more light on this it will be necessary to try and unravel the notion of technological risk perception somewhat further. This is especially relevant for e-voting given the fact that the risk and uncertainty dimension are at centre of most debates.

Science and technology studies have in recent decades made progress on revealing the socially constructed nature of risk perception. Even societies that are similar in

[9] A. Auer and A. H. Trechsel (eds) (2001) *Voter par Internet? Le projet e-voting dans le canton de Genève dans une perspective socio-politique et juridique*, Geneva, Basle, Munich: Helbing & Lichtenhahn. Available at http://www.ge.ch/chancellerie/egovernment/doc/Voter_par_Internet.pdf

[10] See for instance Internet Policy Institute (2001) *Report of the National Workshop on Internet Voting*, www.nsf.gov; also see the California Internet Voting Task Force (2000) *A Report on the Feasibility of Internet Voting* PDF available at www.ss.ca.gov

economic, social and political structures can produce radically diverging conceptualizations and management of risk. Moreover, particularly acute differences –in risk perceptions- are likely to arise when the risk in question touches upon issues that are deemed basic to a societies conception of itself. Could the same be true for e-voting? One of the major puzzles for comparative policy researchers investigating risk regulation is to explain how even given a common base of scientific understanding national variations in risk management persist. A couple of examples of transatlantic divergences on areas such as the environment and biotechnology are illustrative of the phenomenon. With regard to biotechnology very different attitudes exist on either side of the Atlantic in relation to the acceptability of genetically modified organisms (GMO's) even when based on similar scientific evidence.[11]. With regard to the environment striking differences have also been reflected in the policies of the US and the EU with the latter opting for a 'precautionary principle'. Interestingly, what is deemed acceptable evidence in one national policy context is not necessarily given the same weight in another. In other words, differences in the kinds of evidence that a government and the public in general are willing to accept as a basis for policy decisions exhibit marked divergences as do standards of proof and persuasion. Could such insights from comparative policy research apply to e-voting? That is could differences in the tolerance and perception of technological risk influence e-voting arrangements in terms of the mix between the degree of openness and closedness or the extent to which proposals are actually prioritized by the policy agenda?

In seeking to explain differences in science and technological risk perceptions scholars have pointed to the role of framing. The crux of the matter is that framing –

[11] See Vogel, David. Ships Passing in the Night: The changing politics of risk regulation in Europe and the United States. EUI Working Papers, Robert Schuman Centre. 2001(RSC No. 2001/16).

especially when it refers to risk- far from being a neutral statement appears to be the product of deeply engrained cultural belief systems. An example from the so-called e-policy domain can elucidate this phenomenon of 'framing' within a cyber context – and may be pertinent for e-voting. Modern advanced societies increasingly rely on the supply and distribution of certain goods and services, such as water, electricity and telecommunications which are increasingly being tied together by computer networks. There is concern that this reliance on computers and computer networks makes nation's 'critical information infrastructures' vulnerable to 'cyber' attacks. During the nineties the debate in the US concerning critical information infrastructures was couched in terms of a militarist and national security discourse that warned of the potential dangers of an 'electronic Pearl Harbor' and used concepts such as cyberwar and 'information warfare'. The terminology was politically and normatively loaded in favour of a national security approach –with the accompanying advantages that this offered in terms of less public scrutiny and a greater scope for secrecy[12]. The EU on the other hand has opted for a more 'civilian' type discourse –no doubt due to its lack of competencies in the security domain. Recent European Commission documents on network and information security[13] refer to a market failure in the provision of security –most critical infrastructures are owned by the private sector- which makes regulation more palatable. In sum, framing matters. Risks that are acceptable in one social context may be politically more sensitive in others, and it certainly affects the range of policy options considered by policy-makers.

[12] A similar debate has been raging in the US in relation to the recently signed USA Patriot Act (October 2001)

[13] See especially the European Commission's Communication on Network and Information Security: Proposal for a European approach. COM(2001)0298.

One of the big questions in e-voting research is therefore to address how e-voting is being framed in different national contexts? Are there noticeable differences in relation to the degree to which the risk dimension is emphasized or de-emphasized? In spite of a common corpus of scientific and technological knowledge it would not be startling to expect cross-national variations in relation to the tolerance of risk and uncertainty associated with e-voting. Comparative policy research provides countless examples to this effect in other 'e' policy areas.- Thus, in addition to the more obvious factors that may influence e-voting arrangements such as differences in political culture, traditions of democracy and constitutional provisions, divergences in perceptions of technological risk among social groups could also be an important factor in explaining future differences in outcomes.

To summarize, this admittedly very brief survey of the e-policy terrain has identified a series of themes that may be pertinent to the e-vote debate:

- The dialectical tension between 'architecture' and 'politics' and the notion that many of the issues that are raised by e-voting, just as they are in some of the other e-policy domains, are not necessarily new but rather old issues in new guises.
- The inherent tension between opting between open and closed models and the idea that the appropriate mix between the two will be determined by cultural, political and constitutional factors as much as by science and technology.
- A corollary of the former is that we would therefore expect cross national variations in the mix leading to potential variations in e-voting arrangements.

- Finally I have drawn attention to the issue of ‘framing’ and the notion that perceptions of technological risk may vary. Even though we are at an embryonic stage –a key policy community in the US has expressed grave doubts –more comparative research would be required to properly asses its implications for e-voting arrangements in different political contexts.