

E-DEMOCRACY IN DENMARK. Black clouds on a blue sky?

Jens Hoff

Paper presented at a workshop on Internet, Governance and Democracy in Denmark and Asia. Images of Asia Festival. Aalborg University, Denmark, 24 September 2003.

Abstract:

Already in the 1970's and -80's high hopes for democracy were connected with the rise of technologies like cable-TV and digital telephones. This outburst of 'utopian energy' was greatly accelerated with the breakthrough of the Internet in the beginning/middle of the 1990's, and both politicians, IT-developers and many academics depicted the new technologies as almost automatically leading to a new 'golden age of democracy' with increased political participation, better informed and resourceful citizens, better and more transparent political decisions, and a breakdown of religious, cultural and social divisions.

This article will show that in Denmark, as well as elsewhere, these hopes have only to a limited degree been redeemed. Furthermore, global developments related to the development of the digital technological systems have, especially in the aftermath of 9/11, made the coming of a new 'golden age of democracy' even more remote. Thus, with the growing economic and political importance of the Internet, it has increasingly become the object of different kinds of regulation and control, and especially since 2001 there has been a dramatic growth in both state and commercial censorship. In Denmark state censorship has been unknown till now. However, with the recent demand from the Minister of Justice on the public libraries to install filters on their Internet connected computers (notably to prevent citizens from surfing for websites with a pedophilic content) a first step in that direction has been taken. Concerning so-called commercial censorship recent developments within the patent area means that the possibilities of patenting software have been greatly enlarged. Together with the digital rights management systems being built into for example the next generation of Windows, this will enhance the monopolistic powers of the big hard- and software companies, and constitute a company like Microsoft as a new political authority able to dominate considerable parts of the global communications infrastructure.

Thus, the days of seeing the Internet as a free, open and liberal public sphere are long gone. However, this does not mean that there is no room for democratic experiments or developments with computer mediated communication on a local, national or global scale, as long as one recognizes the limits set on these developments by the larger global forces. The article ends by looking at a Danish example of such democratic experiment in the municipality of Odder, and evaluates whether the experiment is able to contribute to local democracy given the global constraints.

Introduction: high hopes for democracy

Already in the 1970's and -80's utopians; especially of an American variety (Etzioni 1975, Toffler 1981, Naisbitt 1982), drew a picture of a future democracy in which democratic dialogue and decision-making would take place through modern communication technology. At that time it was especially the appearance and growth of technologies like cable-TV and digital telephones, which was seen as paving the road for a renewal of democratic institutions and for more democratic forms of participation.

In the 1990's another outburst of "utopian energy" took place (Ilshammer 1997); this time related to the breakthrough of the Internet and its graphical interface "World Wide Web", and a number of authors began to discuss the possibilities for what they called "electronic democracy" or "cyber democracy" (Porter 1995, Rheingold 1993, Hague & Loader 1999). However, a common denominator for the teledemocracy of the 1980's and the cyber democracy of the 1990's was that the point of departure for discussions was most often taken in the technology, or in what it was theoretically possible to achieve with the given technology, not, or only to a limited degree, taking existing political institutions, traditions and cultures into consideration.

But what are the technological features of the Internet, which conditioned such optimism? According to many authors (van de Donk et al. (eds.) 1995, Hoff, Löfgren & Johansson 1999) there are at least seven properties worth paying attention to:

- Increased interaction between participants
 - compared to traditional mass media (newspapers, TV or radio) the new technology contains the possibility of interactivity between sender and receiver of a message. Typical examples are mailing lists, debate fora and chats.
- The declining importance of time and space
 - with the Internet it is possible to access for example the homepages of political organizations or to participate in virtual political debates around-the-clock. Also, territorial boundaries become less important as it is possible to access information and engage in dialogue on a global scale.
- Easier and more equal access to the public sphere
 - compared to traditional mass media the possibilities for "ordinary people" to reach a large audience has been significantly enlarged with Internet technology. It is relatively easy and cheap to create a homepage, and in this way share ones' ideas with other people without the censorship of (state owned or commercial) TV, radio and newspapers. Also, virtual communication is more egalitarian than face-to-face communication as participants do not have to reveal for example their gender, age, ethnicity or social position.
- "All-to-all" communication
 - In contrast to traditional mass media, which are based on the "one-to-all" principle, the Internet creates an environment for "all-to-all" communication.
- Easier access to and control over large amounts of information
 - compared to paper based information modern information -and communication technology (ICT) makes it much easier to find, store and organize huge amounts of information, thus potentially giving the user of such information greater knowledge and oversight capacity than before.
- Possibilities for both "broadcasting" and "narrowcasting"
 - While the Internet is well suited for "all-to-all" communication it is also possible to use it in a more narrow way to either target special groups, or to maintain discussions among such groups.

· Decentralization of control with information

- In contrast to traditional mass media where the control of information is in the hands of state owned or commercial TV-companies or multinational media networks, ICT gives the individual citizen and all types of organizations the possibility of becoming their own editor and publisher, potentially able to reach a global audience.

Thus, the new ICTs; especially the Internet, seemed to create a new political opportunity structure ("affordance" in the word of Hutchby 2003) shifting power away from governments and media monopolies towards citizens and social movements, and at the same time laying a foundation for a more transparent and participatory polity. This impression was underpinned by the virtual presence of a steeply increasing number of organizations of all kinds, some of them especially concerned with democracy and the Internet (e.g. Minnesota E-democracy, the WELL, UK citizens online), and associated or freestanding debate fora. Also, the democratic character of the Internet was stressed by the accounts of how the Net had successfully been used by suppressed groups like the Zapatistas¹ in Mexico or the Chechen liberation movement in Russia to inform about and create global support for their cause, and accounts of how the Net had been used to circumvent state controlled media in for example China in relation to the events on the Tiananmen Square, or in Russia in relation to Yeltsin's coming to power. Furthermore the democratic potential of ICTs was stressed in national ICT-plans like "Info-samfundet 2000" (The Information Society, year 2000; published 1994) and its follow-up "Det Digitale Danmark - omstilling til netværkssamfundet" (Digital Denmark - transformation to the Network Society, 1999), "Vinger åt människens förmåga" (Wings on human capacity, 1994) and "Et informationssamhälle för alla" (An information society for all, 1999/2000); the plans of the Danish and Swedish Governments respectively. Together, all these developments served to cement a myth about the inherent democratic character of ICT. Thus, the more the possibilities of the technology could be unfolded, and the more PC's and Internet could be spread to all corners of society, the more democracy would prevail.

This late 1990s discourse on Internet and democracy led the Danish author Tor Nørretranders to call the Internet: "a successful piece of anarchy" (Nørretranders 1997:7), and the Internet was widely seen as an open, free and liberal public sphere and agora. However, the advent of the millenium seems to have changed all that. Thus, with the growing economic and political importance of the Internet, it has increasingly become the object of different kinds of regulation and control, and especially since 9/11 there has been a dramatic growth in what the Canadian IT-researcher Ronald Deibert (2003) has called state and commercial censorship

In Denmark state censorship of the Internet has been unknown till now. However, with a recent letter from the Minister of Justice Lene Espersen to municipalities and counties commanding their public libraries to install filters on their Internet connected computers (notably to prevent citizens from surfing for websites with a pedophilic content) a first step in that direction has been taken (august 2003; see www.dbf.dk/default.asp?ID=1084). Concerning so-called commercial censorship recent developments within the patent area means that the possibilities of patenting software have been greatly enlarged. Together with the digital rights management systems being built into among others the next generation of Windows, which structure digital communication in a significant ways, this will enhance the monopolistic powers of the big hard- and software companies, and constitute a company like Microsoft

as a new political authority able to dominate considerable parts of the global communications infrastructure.

Below I shall discuss this first Danish step towards state censorship by looking at the effects of the known filtering technologies. Secondly, I shall look at what commercial censorship means for different aspects of democracy, and finally I shall look at some countervailing evidence: an example of a successful democratic experiment in a Danish municipality.

State censorship in Denmark?

As mentioned, Deibert (2003) points to the fact that the Internet has increasingly become the object of state and commercial censorship. Actually, he points to three set of actors who are struggling to control the Internet in a complicated form of governance: the nation states (and the EU), big multinational hardware, software and telecommunications companies and media conglomerates, and civic networks/NGO's which specifically aim at influencing the global communications policy (e.g. Association for Progressive Communications, Computer Professionals for Social Responsibility, Human Rights Watch, Reporters Without Borders). To this should be added two more sets of actors. Firstly, a couple of private, non-profit organizations, who have been licensed to control, or set themselves up to build, specific features of the Internet. Most notable here is ICANN (the Internet Corporation for Assigned Names and Numbers), established in 1998; an organization, which coordinates the assignment of Internet domain-names, IP-addresses and protocol parameters. Also the organization is in charge of coordinating the maintenance of the Internets backbone server architecture. Another important organization is W3C (World Wide Web Consortium), which develops inter-operative technologies (specifications, guidelines, software, etc.) meant to further the technological development of the Internet. The W3C-team is lead by Tim Berners-Lee, who is regarded as the "inventor" of the Internet. Secondly, the United Nations has recently become a player in this field through its arrangement of the first World Summit of Information Technology (WSIS) held in Geneva in June 2003 (based on UN resolution 56/183). The main aim of the UN involvement in the field is to find means to bridge the digital divide between North and South, and to find ways to create access to the global information infrastructure for the peoples of less developed countries. To reach this goal the collaboration of governments, civil society, business and international organizations is sought, and at the moment a series of so-called PrepCom (Preparatory Committee) conferences are taking place in order to finalize the WSIS Declaration of Principles and Plan of Action (see www.wsis.org or www.una.dk/wsis).

Focusing first on state censorship it is well known that many totalitarian regimes censors Internet content by installing filters at the server-level to control users' access. In a 1999 report from Freedom House, a free speech organization, 45 countries were identified as censoring Internet content; among these Aserbajdsjan, Cuba, China, North Korea, Iran, Iraq, Saudi-Arabia, Syria and Vietnam (see Staksrud 2002).

However, the use of filters and filtering techniques is only one out of a number of ways in which nation states try to regulate the Internet. Other strategies are: 1) laws regulating this new area of mass communication, 2) self- or co-regulation by/with the Internet industry through the use of commonly agreed ethical rules, 3) use of hotlines to fight especially pedophilic content, and 4) information campaigns. Here I will focus on the question of filters and filtering techniques, as this is what is currently at stake in Denmark. The

point of departure for the discussion will be filters developed in the US, as they dominate the market today.

Generally one can say that what filtering programs do is that they compare parts of or a whole data-file (for example a newsgroup, a document or a website) with a pre-defined set of rules. The result of the comparison determines whether the user will be allowed to receive and view the file on his/hers computer. Common rules for filtering are:

- Blocking of certain files or websites by comparing their URL, name or IP-address with a list of forbidden files or websites (blacklisting)
- Blocking all files except already accepted files or websites (white listing)
- Filtering of chosen files/websites by comparing their content with a list of words, word combinations or other identifiable elements (for example degree of nakedness)
- Filtering of chosen files/websites by comparing a classification mark associated with the file/website with a predefined set of classification criteria.

The two first types of blocking require that a person has evaluated each file/website and decided whether it should be either black- or white-listed. The third type of filtering requires that a person defines the list of forbidden words or word combinations, but the selection itself is automatic. The last form of blocking demands that persons establishes classification criteria and then marks every file and website. After the marking files/websites can be filtered according to given criteria. The classification takes place through the content providers or a third party, for example a government body, and is a prerequisite for many filtering programs.

Some of the best known filtering programs are: Cyberpatrol, CYBERSitter, Net Nanny, SurfWatch, BAIR and Safesurf. However, it has been disclosed by among others Peacefire, an organization fighting for children and youngsters right to information and freedom of speech, that all of these market-leading filters have blocked information that should not have been blocked according to their own rules. Thus, Cyberpatrol has blocked student organizations at certain American universities, UseNet discussion groups like alt.journalism and soc.feminism. CyberPatrol also for a considerable amount of time blocked Electronic Frontier Foundation and HotWired. Also, the organization Planned Parenthood is blocked. Net Nanny block newsgroups with information about AIDS, women organization and equal rights organizations like soc.feminism, alt.feminism and the National Organization for Women in the USA. Furthermore it has been documented that during the elections in the USA in 2000 a number of candidates; both Democrats and Republicans had their websites blocked by CyberPatrol.

Elisabeth Staksrud (2002), in her article from where I have most of the above information on commercial filters, concludes that as the known filters have such obvious errors, they risk making matters worse than before. Firstly, by creating a false sense of security, as one is led to believe that children and youngsters are protected by these filters. Secondly, because important value choices are made by the producers of the filters. When women organization, some politicians and proponents of free speech are blocked, this

is a form of political censorship being imposed on a market with little knowledge of what is going on.

Thus, when the Danish Minister of Justice tries to force public libraries to install filters on their Internet-connected computers in order to refrain citizens from surfing for websites with a pedophilic content, this is a policy which is not only likely to be quite ineffective with the known filtering technologies, but also a policy which is likely to limit access to information and legitimate expressions of free speech. It is a type of symbolic control policy, which is harmful to democracy. Hereby it is sadly in line with for example policies in the USA demanding the use of commercial filters in schools and public offices (Staksrud 2002:77).

Commercial censorship

With the concept "commercial censorship" Deibert (2003) denotes the different ways in which commercial actors tries to influence and dominate the Internet. In our kind of societies most of these practices are of course 100% legitimate and normal. However, as I shall try to illustrate, a number of existing and especially emerging practices seem to have properties that impinges on issues like access (in the broadest sense), privacy, diversity and openness in a negative way, thereby undermining important aspects of democracy.

There are at least five strategies that commercial actors use in trying to maximize their profits when dealing with ICT, in particular the Internet: 1) to become market leaders (set de facto standards; examples are Microsoft (Office, Internet Explorer), Oracle (databases) and Adobe (pdf-files), 2) work in international standards organizations to set de jure standards (CEN, ETSI, IEC2), 3) to take out patents (on hardware, software), 4) to register copyright on their products, and 5) to ensure copyright protection by developing digital rights management systems.

Here I shall deal only with recent developments within the copyright and copyright protection area, and the software patent area, as it is especially developments within these areas, which are of democratic concern at the moment.

Concerning copyright we know that with the digitalization of a wide range of consumer products, including movies, music and books, pirate duplication and distribution has become a problem. Companies in the affected industries such as the recording industry and the motion picture industry have claimed large losses in potential sales, even though determining exact figures is very difficult. It is therefore not surprising that the involved companies and their associations such as the RIAA (Recording Industry Association of America) and the MPAA (Motion Picture Association of America) have taken increasingly stronger measures to protect their property and preserve copyright in cyberspace. Naturally, there are good reasons to support copyright measures because without a system to protect against theft and plagiarism and to ensure appropriate compensation for expended resources, the circulation of ideas central to liberal democratic society could wither. However, the problem seem to be that in cyberspace it is difficult in practice to apply the longstanding principles of protection of intellectual property, and that the measures taken seem to have a number of unintended consequences, among these restrictions on creativity and self-expression. Most bothersome from a democratic perspective is, however, the development of so-called digital rights management systems (DRM-system), which works on the basis of codes built directly into the communications media themselves (for example into the motherboard of PC's).

If we look first at one notorious example of copyright protection, the Digital Millennium Copyright Act, an act passed by US Congress on October 28th 1998, it has been shown in a study by the Electronic Frontier Foundation that the act has been employed as a tool for anti-competition, that it has stifled legitimate research into cyber-security and encryption technologies, and that it has undermined "fair use" of products. It has also impinged on academic databases and electronic journals restricting their use, and many believe that the act will put restrictions on academic work in the public domain (see: www.law.duke.edu/pd/papers.html#history).

We could console ourselves with the fact that the Digital Millennium Copyright Act (DMCA) is only an American law if it was not for the fact that similar heavy-handed laws are being adopted in a number of other countries. Also, the US is pushing the DMCA in bilateral trade negotiations, and many of its elements are manifest in treaties administered by the World Intellectual Property Organization (WIPO).

However, more concerning from a democratic point of view are the measures currently being taken to protect intellectual property and copyright through technical means; in particular the attempts to build codes into software and hardware to structure permissible communications. Most notable in this respect is Microsoft's Palladium system and the work going on in the so-called Trusted Computing Software Alliance (TCPA); an organization set up by Intel, IBM, Microsoft, HP and Compaq, but which today comprises more than 100 IT-firms.

Palladium3) is a further development of Microsoft's existing DRM-system, which works for sound- and video files in Microsoft's Media Player. A recording company or a video producer who wishes to control the use and copying of the product on the buyer's computer can use Microsoft's Media Player. With software from Microsoft the producer can change the sound- or video files to encrypted files, which can only run on Media Player if the user has a digital key, which the user has to buy. The producer can regulate the number of times a tune can be listened to or a video can be shown, and whether the sound- or video file can be copied or burnt on a CD. This system is very similar to other DRM-systems, also those developed on open source platforms. However, a major difference is that Palladium generalizes the DRM-system, so that the whole operating system on a given PC will be controlled by a system of rights, where not only sound- or video files, but also e-mail, databases, text, pictures and other programs, are protected against unauthorized use.

If things turn out as Microsoft expects, Palladium will be the standard operating system on the next generation of computers. Seen in the context of the market dominance of central Microsoft products like the Office package and Internet Explorer, Microsoft will be able to decide which programs it is possible to run together with its dominating products. If Microsoft programs are used on the big majority of the citizens' computers it means that Microsoft will obtain the possibility of denying other programs access to data protected by Microsoft programs. Thus, Microsoft will have a crucial influence on which programs it will be possible to run on the computers. If, therefore, the most important information/content providers in society accept Palladium, it forces citizens to also use Palladium if they want to buy text-, sound-, or video files, or if they want to send and receive protected e-mails and other information from for example public authorities. Microsoft claims that one of Palladium's big advantages is that the user can avoid viruses etc. because only accepted programs can run under Palladium. However, the same functionality can be obtained by IBM's TCPA-system for Linux. The crucial difference is that while

IBM gives the owner of the PC a possibility to protect himself against "foreign" attempts to change the software on the computer, Microsoft is protecting the "foreign" content providers against the owner if he/she attempts at making changes to his/hers PC.

That this is not a technological fairy tale is evident by the WIPO and EPO4) patent applications sent in by Microsoft in order to patent their DRM and TCPA-systems. In December 2001 Microsoft got a US-patent on a "Digital Rights Management Operating System", which is likely to be used to block competing DRM operating systems, ensuring Microsoft's the position as the only provider of DRM-systems.

Thus, the coming of the DRM-systems should be seen in connection with the development in the area of software patents, and it is exactly the combined development that makes the situation very problematic from a democratic point of view.

To cut a long story very short there has for some time been a big difference in the American and the European approach to software patents. Whereas it has not been possible to patent software in neither Denmark nor the rest of Europe, software patenting has been possible in the USA. However, the EPO has now changed its practice and made a reinterpretation of the European Patent Convention so that it is possible to patent most software that can be run on a computer (given that it is new, and can be characterized as an "invention").

To make matters worse a new EU Directive, which is being negotiated in the European Parliament at this very moment (September 2003), will force the EU countries to pass legislation, which widens the field for software patents even more than the new practice of the EPO. If the Directive is passed this will bring the European situation very close to conditions in the USA5)

But what is wrong with software patents? Isn't it just a legitimate compensation for the costs of developing new products, and isn't the reward of a patent a necessary incentive for innovation? This is a long discussion which is outside the scope of this paper, but a number of authors among these Hart, Holmes & Reid (2001), and Bjerke (2003) has convincingly shown that software is a special type of product, the patenting of which will have a number of negative consequences. Firstly, software patents seem to primarily protect the market position of dominating firms more than stimulating innovation. Secondly, institutions - also public institutions - will loose the right to know about what is going on in their IT-infrastructure as most of the programs they will be using will have closed code. Thirdly, access to the Internet and other forms of digital exchange of information requires common standards. With the new patent regime it will be possible to patent such standards. If this happens paying a fee to use the Internet is a very likely prospect. Also, this can mean that it will be difficult to protect oneself against possible secret tapping of information. Returning to the next generation of Windows, the Palladium system again, Microsoft is likely to, through the combination of patented Microsoft standards, and the dominance of Microsoft programs on many citizens' computers, get a crucial influence on the type of programs required to read the lions share of the information on the Internet. A worst-case scenario is that also search engines will have to be certified by Microsoft before citizens can make use of them. In this way Microsoft and its partners will obtain a crucial power to decide about what it is possible to distribute over the Net and what not - a power which is very reminiscent of a censoring function. Also, Microsoft will get the possibility to

tap computers for information, and this goes for citizens, businesses and public authorities. This seems in itself to be reason enough to seriously reconsider the pending EU Directive on software patents, and to make sure that open source alternatives to Palladium exists. It is true of course, that citizens, businesses and public authorities will get better possibilities of controlling their internal communication with Palladium, and be able better to avoid hacking etc. But insofar as it will be Microsoft who is checking the fundamental identity of both hardware and software, citizens will have to get this identity certified regularly by Microsoft. In fact, this is already happening today with Windows XP (Jennings 2003). This creates a way for Microsoft to access the citizens' data, and as also the information activities of criminals and terrorists will be protected by Palladium both police and intelligence services will be likely to try to obtain information through a collaboration with Microsoft.

Thus, as a conclusion we can say that if Microsoft gets away with patenting Palladium, this will give Microsoft both a legislative power (control over programs and access to information), a judicial power (it will judge about violations), and an executive power (it can block access to information) of enormous dimensions, in a world where computers and the Internet, at least in the rich part of the world, are increasingly citizens' access to news, entertainment, information, products of various kinds, jobs, private communication, etc. This power, which is furthermore highly automated, will set Microsoft up as a very significant political authority in the information society.

Summing up, concerning these examples of state and commercial censorship what we see is a serious undermining of the Internet as an open, liberal and free public arena. Gradually limitations on access in the widest sense as both free access to different kinds of hardware/software and information, on privacy, on diversity and on openness have been or is being imposed. This infringement on the Internet as a symbol of liberal democracy is happening in the shadow of "the war on terrorism", and the Internet might be seen as one of the bigger casualties of this war.
Is there still hope for democracy? : A local Danish experience

Deibert (2003), in the article referred to a couple of times above, also paints a very bleak picture of the possibilities of using the Internet for civic democratic communications, and of its becoming a truly democratizing force. However, he sees some hope in the forces that are currently fighting censorship and surveillance on the Internet; forces which he identifies as civic networks. Some of these are well known such as the APC (Association for Progressive Communications), Human Rights Watch and Reporters Without Borders. He also seems to invest some hope in progressive elements in the hacker community, for example an activist group like Hactivismo.

While Deibert is basically referring to a North American context, the situation might be somewhat different in Europe. In some EU countries like France and Germany it is becoming official policy to reduce the dependence on Microsoft product. In Germany 20% of the public administration has now migrated to open source products, and the German Ministry of Interior has developed a migration plan that all public institutions can follow. Also the EU is devoting considerable sums of money to develop open source products in its 6th Framework Program. (It is ironic of course that this runs counter to the policy resulting from the pending directive on software patents, and maybe even more from the practice of EPO (see footnote 5)). Furthermore, in quite a lot of EU countries political/public institutions have tried to employ ICT for

democratic purposes, some of these experiments and products being supported by the EU. In Denmark such experiments and developments have especially taken place at the municipal level.

Here I am going to refer to what I consider a particularly successful case, namely the case of the so-called OdderWeb developed in the municipality of Odder. Odder is an average size Danish municipality with around 20,000 inhabitants located in Eastern Jutland just south of Aarhus; the second largest Danish city. Concerning citizens' income and education it is a little above the national average. Internet diffusion in the municipality is high, and believed to be above the national average of 70% of households (77% including home and work, figures for first 6 month of 2003; see Danmarks Statistik 2003. Exact figures for Odder are not known). The municipality has been one of the most ambitious municipalities in Denmark in trying to develop ICT solutions for both administrative and democratic purposes, and the official homepage of the municipality has been rated among the top-five in Denmark for two consecutive years in the annual "Best on the Net" ratings done by the national Board of IT and Telecommunications.

The homepage of the municipality (www.odder.dk) is a neat and orderly homepage with information about municipal activities, culture, children and youngsters, education, health and care, housing, tourism, business opportunities, jobs, shopping, etc. It carries interactive services such as a debate forum, possibilities for contacting municipal politicians, for complaining to municipal authorities, for participating in nationwide debates, etc. It also has some transaction services such as E-boks (a personal archive for official, electronic documents, bank statements, etc.), the possibility for electronically changing to another physician, the possibility of electronic payment of municipal bills, etc.

However, most interesting from a democratic point of view is probably the so-called OdderWeb, which is an application, developed by the small local IT firm Kubus Clevernet Aps. OdderWeb is accessible from/integrated with the municipal homepage but its unique characteristic is that it functions as a "private room" on the Internet; a dynamic and easy-to-use homepage which is accessible only with a private "key" (login). However, once opened one can decide to make the whole homepage, or parts of it, accessible for everyone. On the homepage one can upload family pictures, shopping lists, e-mail addresses, enter events in a calendar, keep a log, etc.; functions which can be accessed from anywhere on the Net. However, apart from this "private room" it is also possible to create groups or communities on the homepage with friends, fellow joggers, to create a virtual classroom with schoolmates and teachers, etc. The integration with the municipal homepage also means that one can subscribe to different types of news from municipality, and have them arrive directly in ones' own electronic mailbox. Thus, the unique feature of OdderWeb is that it integrates functions for private use, for citizen-to-citizen (C2C) communication, and for citizen-to-administration (C2A) interaction in one web application. The thinking behind the application, disclosed around the opening of OdderWeb February 25th 2003, is that by offering citizens an easy-to-use "private space" on the Internet, the municipality will stimulate citizen interest in using the Net, and at the same time improve citizens' proficiency in ICT. This is thought to lead also to an increased use of ICT in interactions with the municipality; thereby enhancing both efficiency and democracy in the municipality.

Concerning the democratic effects the author was, at the opening of OdderWeb, invited to present a proactive evaluation of the possible

democratic effects of the application. In so doing I used 10 criteria for a (normative) democratic evaluation of digital applications for political communication developed in Hoff (2000) and in Hoff, Löfgren & Johansson (1999). These criteria are criteria derived from a more traditional view on democracy, as a "parliamentary chain of steering" (the Whitehall-model), as well as from a view that recognizes the tendencial shift in our societies in the direction of governance (March & Olsen 1995). The 10 criteria are: 1) ability for citizens to influence politically (strengthening/weakening), 2) stimulation of public debate in relation to political decisions (positive/negative effect), 3) whether the municipal boards' capacity to act is increased or not? (yes/no), 4) whether the responsibility and accountability of the municipal board is increased or not? (yes/no), 5) whether the responsibility and accountability of the municipal administration is increased or not? (yes/no), 6) whether citizens become more politically active and responsible? (yes/no), 7) whether there is a positive development in citizens' democratic identities? (yes/no), 8) whether there is a positive development of citizens' political resources and competencies? (yes/no), 9) whether we see a development of relevant narratives on policies and politics (positive stories of possibilities for political community, influence, change, etc.) (yes/no), and 10) whether the local political system becomes more flexible in its approach to citizens' wants.

In my proactive evaluation I judged OdderWeb to have a possible positive impact on 5-6 of these dimensions, and none or an uncertain (but not negative) impact on the other 4 dimensions. Thus, OdderWeb was estimated to have a positive impact on dimensions no. 6 to 10, and a more uncertain positive impact on criteria no. 2 (public debate). So according to this admittedly raw and premature judgement, success was inscribed in OdderWeb from the beginning. And indeed, within some months more than 800 citizens had established their "private room" on OdderWeb equaling around 10% of households with Internet access in Odder.

However, given the global developments described above one might wonder how long the democratic idyll in Odder, as well as elsewhere, might last? What happens to the C2C and C2A networks and communication/transactions if and when Palladium hits Odder? Will the municipality be able to continue to provide for users of open source software? If not, who will be included and who will be excluded from this part of the local political community? And what will the municipality do about that? These are just some of the questions that springs to mind; questions of a character that we will be increasingly confronted with in the near future.

Conclusion

There are two important lessons to be learned from the analysis above of state and commercial censorship, and of the democratic experiment with ICT at the municipal level in Denmark referred to. The first one is that it is becoming increasingly impossible to separate local and global developments especially in relation to ICT. This of course is what globalization is all about, but the developments described above illustrates very clearly that this is also the case when it comes to politics. As Deibert says: "From now on it is all world domestic politics" (2003:1). Therefore, work for use of the Internet to improve local democracy has to be connected with the work to avoid both state and commercial censorship on a national and a global scale. If not, we risk seeing that both freedom of information (i.e. the right to inform, and to be informed) and personal control over one's own computer (privacy) is seriously diminished.

The second lesson to be learned is that the architecture of the Internet should not be taken for granted. This point has been put forward forcefully by Lawrence Lessig (2000), but today it is clearer than ever before that politicians, public employees, citizens and social scientists can no longer refrain from dealing with so-called "technical issues" as such issues are of enormous economic and political importance. Also, computer scientists, system administrators as well as hard-and software companies can no longer avoid taking ethical and political standpoints on how they want to see their technology being used, and who is should benefit.

References:

Bjerke, F. (2003): "Softwarepatenter og magt" in Hoff, J. (ed.): Danmark som informationssamfund. Muligheder og barrierer for politik og demokrati. Aarhus Universitetsforlag: Aarhus (in print).

Castells, M. (1997): The Power of Identity. Blackwell Publishers: Massachusetts & Oxford.

Danmarks Statistik (2003): Informationssamfundet Danmark 2003. Copenhagen.

www.dst.dk/pukora/epub/upload/5425/kapitel3.pdf

Deibert, R. (2003): Black Code: Censorship, Surveillance, and the Militarization of Cyberspace. Paper prepared for the International Studies Association Conference, Portland, Oregon, USA. February 2003.

Etzioni, A. (1972): "Minerva. An Electronic Town hall" in Policy Sciences:3, pp. 457-74.

Forskningsministeriet (1994): Info-samfundet år 2000. Rapport fra udvalget om Informationssamfundet år 2000. København.

Forskningsministeriet (1999): Det digitale Danmark - omstilling til netværkssamfundet.

<http://www.detdigitaledanmark.dk/rapport/ddd.pdf>

Hague, B. & Loader, B. (1999) (eds.): Digital democracy. Routledge: London & New York.

Hart, Holmes & Reid (2001): The Economic Impact of Patentability of Computer Programs.

http://europa.eu.int/comm/internal_market/en/indprop/comp/studyintro.htm

Hoff, J., Löfgren, K. & S. Johansson (1999): Internet og demokrati. Erfaringer fra kommunalvalget 1997. Jurist- og Økonomforbundets Forlag.

Hoff, J.: (2000): "Technology and social change: the path between technological determinism, social constructivism and new institutionalism" in Hoff, J. Horrocks, I. & P. Tops (eds.): Democratic Governance and New Technology. Technologically mediated innovations in political practice in Western Europe. Routledge: London.

Hutchby, I. (2003): "Affordances and the Analysis of Technologically Mediated Interaction: A Response to Brian Rappert" in Sociology, Vol. 37(3):581-589.

Ilshammer, L. (1997): Demokr@ti - det elektroniske folkstyrets muligheder og problem. (SOU 1997:23). Justitiedepartementet, Fritzes Forlag: Stockholm.

Jennings, M. (2003): Windows XP Shows the Direction Microsoft is Going.

<http://www.hevanet.com/peace/microsoft.htm>

Lessig, L. (2000): Code and other laws of Cyberspace. Basic Books: New York.

March, J.G. & Olsen, J.P. (1995): Democratic Governance. The Free Press: New York.

Naisbitt, J. (1982): Megatrends: Ten New Directions Transforming Our Lives. Warner Books: New York.

Nørretranders, T. (1997): Stedet som ikke er - Fremtidens nærvær, netværk og Internet. Aschenhoug: København.

Porter, M. (1995): "Cyberdemocracy: The Internet and the Public Sphere" in Holmes, D. (ed.): Virtual Politics: Identity and Community in Cyberspace. Sage Publications: Whiltshire.

Proposition 1999/2000:86. Et informationssamhälle för alla.

Rheingold, H. (1993): "A Slice of Life in My Virtual Community" in Harasim, L.M. (ed.): Global Networks - Computers and International Communication. MIT Press: Cambridge, Mass.

SOU 1994:118. Vingar åt människans förmåga. Betänkanda från Informationsteknologikommisionen. Stockholm. Fritzes.

Staksrud, E. (2002): "Ytringsfrihet og sensur på Internett. Politisk regulering og kommersiell filtrering" i T. Slaata (eds.): Digital makt. Informasjons- og kommunikasjonsteknologiens betydning og muligheter. Gyldendal Norsk forlag: Oslo, pp.64- 94.

Toffler, A. (1981) (org. 1980): Den tredje bølge. Erichsen: København.

Van de Donk, W.B.H.J. et al. (eds.) (1995): Orwell in Athens: A Perspective on Informatization and Democracy. IOS Press: Amsterdam.

Internet resources:

Dansk Biblioteksforening: www.dbf.dk/default.asp?ID=1084

World Summit on Information Technology: www.wsis.org

- Danish information on WSIS: www.una.dk/wsis

1) Castells (1997:68ff) even call the Zapatistas the "First Informational Guerilla Movement".

2) CEN is an acronym for European Committee for Standardization, ETSI is an acronym for European Telecommunications Standards Institute, and IEC is the International Electrotechnical Commission.

3) The following information on Microsoft's Palladium system is all from Bjerke (2003; in print).

4) WIPO is the World Intellectual Property Organization, and EPO is the European Patent Office.

5) Concerning the EU Directive on Software Patents the thrust of the directive was changed through a very active intervention by the open source movement in a number of European countries. The directive now states that it is only possible to patent software, which steers hardware use, but that all other types of software cannot be patented. However, the directive still need to pass the Ministerial Council, and might therefore still be subject to a watering out. Also, the practice of the EPO has become very lax in this field, probably due to pressure from big business.