5. Digital Citizen Rights

This case study on digital citizen rights (DCR) is necessarily of a different nature to the other cases of this project, for two reasons. First, our research found that the very concept itself is of an amorphous and evolving nature. Different interlocutors in the developing debate over how to incorporate the “digital” into existing rights frameworks often emphasise very different things. For some, DCR would include general Internet rights such as freedom of speech and censorship, which we exclude from this case study. Second, the subject of the study is not concerned with a particular type of eGovernment programme – one in which a specific service is digitised, to greater or lesser effect. Instead, it is cross-cutting, and potentially touches on issues relevant to all types of eGovernment provision. The essence of the DCR case presented here is an analysis of normative claims regarding what the state should and should not be engaging with in the digital era. This potentially impinges both on the sorts of programmes that governments implement, and on the ways in which they do so.

In response to these two distinguishing features of DCR, the case study presented below is structured accordingly. We begin by providing an extensive analysis of both the historical precursors and the current emerging contenders in the sphere of digital rights claims. From this analysis, we show that a number of distinct strands can be identified in the developments, and that these strands have received very different degrees of attention among participants in relevant debates.

As a result of the perceived importance of the most long-standing strand – the one that we associate with T.H. Marshall's “civil citizenship”– we then move on to develop a conceptual framework that can be used to delineate different aspects of DCR in this area. The typology that emerges from this work is one built upon an idea of information rights. It allows us to delineate the different types of legislation and rights claims that are applicable to DCR.

With this typology in hand, we move on to an empirical embedded case study. We identify Denmark as a leading exponent of DCR adoption, and set out the results of field research conducted during a visit to Copenhagen. The aim is to present evidence as to how rights issues have affected real-world eGovernment initiatives. The results suggest that the newer rights claims identified in the preceding section have had little influence on eGovernment in Denmark – both from state and civil society perspectives.

The case study is then concluded with a discussion of the key lessons that can be drawn from the historical, conceptual, and empirical sections.

Digital Citizen Rights: what should they entail?

We carried out a selective survey of the emerging field of rights statements and claims in the area of Digital Citizen Rights (DCR). While initially slow to acknowledge the implications of the digital era for citizen rights, a range of proposals have recently been forthcoming from governments, scholars, and activists. Whether acknowledged or not, these new normative claims tend to share a heritage of earlier, non-digital, international rights declarations. Consequently, we begin our survey with a brief outline of the important features of these statements.

The picture that emerges is one of an evolving field that has been influenced at all levels of human endeavour. Important contributions have been made by large-scale international agreements between governments, by individual national governments, by communities of pan-European local governments, and by provident individual scholars.

However, despite these contributions, the picture is also one of an under-development. For their many worthy and eminent additions to our understanding of rights as they relate to “digital citizens”, it must be questioned how large an impact this community of actors has really had on public policy. This may partly be explained by the lack of legal enforceability that characterises most of the expressions of digital rights that we discuss below. They tend to fall into the category of aspirant rather than applied practice. Nonetheless, it is reasonable to see them as important steps in a process of political and civic awakening as to the implications of our onward march into the digital era.

Precursors

In this section, we set out a history of some of the prominent historical precursors to the more self-consciously “digital”rights claims that have been proposed recently. With the aim of both brevity and authority, we concentrate only on five international treaties and declarations that form foundational parts of the recognised body of international human rights law. These are the Universal Declaration of Human Rights (UDHR) (United Nations 1948), the European Convention on Human Rights (ECHR) (Council of Europe 1950), the International Covenant on Civil and Political Rights (ICCPR) (United Nations 1966), the International Covenant on Economic, Social and Cultural Rights (ICESCR) (United Nations 1966b), and the Charter of Fundamental Rights of the European Union (CFREU) (European Union 2000).

For our purposes here, we choose to highlight two aspects that emerge from this body of international legal instruments. First, is the well-recognised idea of individual privacy. It is referred to explicitly in numerous international declarations, and has gone on to find statutory force in most “developed world” jurisdictions. Second, and somewhat more controversially, we discuss the degree to which these legal instruments have embedded within them, an implied notion of a right of access to knowledge or information. To the extent that they do, we can see them as important forerunners to many of the later, more specifically “digital”, rights assertions.

Privacy

Privacy has a long history of recognition in instruments of international law, and it is easy to see how those earlier assertions of such a right have important implications in the digital era. The added scope that interlinked databases provide for the sharing and aggregation of data on individuals clearly generates the potential for a reduction in privacy.

Of course, to some extent, these earlier privacy declarations reflect their times. With the prevailing technological constraints, it was not possible to monitor the communications and transactions of entire populations. Thus, the privacy assertions tend to be framed in terms of individuals facing specific, physical intrusions by the state. We can see this in Article 12 of the UDHR (UN 1948), Article 8 of the ECHR (Council of Europe 1950), and Article 17 of the ICCPR (UN 1966).

> *[UDHR] Article 12*
>
> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*
>
> *[ECHR] Article 8 – Right to respect for private and family life*
>
> *Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *[ICCPR] Article 17*
>
> *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*

The onset of technological change led to adjustments to the expression of the privacy principles that underlie the articles above. In the European Union, data protection had already found legislative

form in Directive 95/46/EC (EU 1995) which set down a framework for "the protection of individuals with regard to the processing of personal data and on the free movement of such data".

In 2000, the EU adopted the Charter of Fundamental Rights of the European Union (EU 2000), and there we see a more expansive notion of privacy rights expressed.

> *Article 7 – Respect for private and family life*
>
> *Everyone has the right to respect for his or her private and family life, home and communications.*
>
> *Article 8 – Protection of personal data*
>
> *Everyone has the right to the protection of personal data concerning him or her.*

Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

While Article 7 maps onto those of the earlier documents, Article 8 clearly pushes forward the boundaries of privacy rights. It provides recognition for the implications of the changing scope of technical possibilities. The removal of physical limitations to the collection, retention, and analysis of personal data can be seen to herald the arrival of equivalent legal limitations.

One striking aspect of rights associated with privacy is that they tend to be inherently limiting on the actions of the state. Restrictions are placed on what information can be collected and stored, and even on the ways in which information can be linked together – "data must be processed fairly for specified purposes". Those privacy rights that do not constitute limitations on the state very often amount to duties on it instead. So, once the data is collected, it must be possible for the citizen to inspect and correct the information that is held. Linking our discussion here back to the broader project, the very nature of privacy rights, to the extent that they influence eGovernment projects, would seem to offer only the prospect of additional barriers. However, as we shall see in our other embedded case studies, this conclusion turns out to be overly pessimistic.

Access to Information

In contrast to the potentially negative relationship that can be discerned between eGovernment and privacy, another manifestation of DCR appears likely to have a more benign impact on the structure and development of government on the web. The assertion of rights of "access to information" hold the promise of imposing duties on the state to make information available in a way that citizens can easily find and use. Internet technologies offer the most obvious mechanism for achieving these aims in an efficient manner, and thus rights of access to information may well be enablers to eGovernment.

But is there a right of access to information? International law holds numerous provisions that indicate that there is. Article 19 of the UDHR, Article 10 of the ECHR, Article 19 of the ICCPR, and Article 11 of the CFREU all provide for freedom of expression and the right to receive and impart information. Each is founded in the notion of freedom of opinion and expression. However, from the point of view of access to information, these articles appear to be rather weak. They amount to little more than a requirement of non-interference – by the state or otherwise.

The ICESCR goes a step further, though. It imposes a positive duty on the state to make it possible for all people to participate in cultural and scientific progress.

> *[ICESCR] Article 15*
>
> *The States Parties to the present Covenant recognize the right of everyone:*
>
> *To take part in cultural life;*
>
> *To enjoy the benefits of scientific progress and its applications;*
>
> *To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.*

The steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for the conservation, the development and the diffusion of science and culture.

Thompson (2006: 48) is bold in his assertion that the body of international law discussed above constitutes a strong source for a right of access to knowledge. He claims that,

> *even though the right of access to knowledge is not directly acknowledged in any of the dispositions of those instruments, it is an indispensable tool for the realization of the rights provided for by many of them. In this sense, we could say that the right to access at the same time underlies and distinguishes itself from the rights entrenched in the ICCPR and the ICESCR. The right of access to knowledge, as generally affirmed, is not the right to culture, is not the right to education, is not the right to freedom of information, is not the right to food, is not the right to health, and at the same time is at the background for the fulfilment of all of them – it is as basic and as essential as a right to have rights.*

Even if we do accept claims of this nature, it is possible to question the extent to which they will or should apply to eGovernment. Does a right of access to information, justified in the way above, constitute a duty on the state to make available the information that it holds? A case for such a proposition can be seen to rest on ideas of equal participation in the cultural and political aspects of the state. If state-held information is only available to the few, then equitable participation by all will likely be impeded.

Whether the reader accepts an argument of this form, or indeed any other, should not distract from the core purpose of this section. In a brief way, we have only sought to set out the legal antecedents to the emerging field of digital rights frameworks. It is to these that we now turn.

Emerging Digital Rights Frameworks

In this section, we provide a selective survey of more recent, and more overtly "digital"-oriented, rights statements and claims. We discuss the features of four such projects, each of which has had quite a different impact on the continuing debate in this area.

World Summit on the Information Society (2003-2005)

The World Summit on the Information Society (WSIS) was a UN organised process that, following its endorsement in 2001 by the UN General Assembly, constituted two phases: Geneva (2003) and Tunis (2005).[131]

> *The objective of the first phase was to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake.*

As such, its relevance to the recent development of DCR is clear. Indeed, discussing what they term the "global information society", Drake & Jørgensen (2006: 4-5) see the WSIS process as an important step towards uniting the previously disconnected worlds of ICT policy-making and human rights.

Following a three day conference in Geneva in which 11,000 delegates, from 175 countries participated – including heads of state and government – a Declaration of Principles was agreed.[132] This declaration identified a number of "key principles" for an "information society for all". While much of the focus of the declaration is on development issues with respect to poorer parts of the

[131] http://www.itu.int/wsis/basic/about.html (accessed 2007/04/06).

[132] We concentrate our analysis on the Geneva Declaration rather than the Tunis Commitment. This is not to downplay the important of Tunis – indeed, Drake & Jørgensen (2006: 33) cite phase 1 as "human rights damage control", while phase 2 was "essentially different in this regard". However, in the areas of direct interest to us here, the Geneva Declaration is both more extensive and clearer in its expression of the important principles that are at the foundation of the WSIS process.

world, some aspects are nonetheless of relevance to rights issues surrounding eGovernment in the developed world. At the most basic level, the WSIS declaration offers a highly prominent successor, in the area of information policy, to the international agreements already discussed above.

Of the 11 "key principles", the most relevant for our purposes are:

1. "Information and communication infrastructure: an essential foundation for an inclusive information society"
2. "Access to information and knowledge"
3. "Capacity building"
4. "Building confidence and security in the use of ICTs"
5. "Ethical dimensions of the Information Society"

From this list, the fourth and fifth principles emphasise the importance of privacy as a fundamental underpinning of any "information society". Interestingly, while the latter invokes privacy as a fundamental right, the former amounts to an instrumental justification. That is, "building confidence and security in the use of ICTs" is seen as a necessary step to encourage take-up of digital services – where such services are seen as a positive end in and of themselves.

The first principle in the list above is a declaration of the importance of access to technology, and particularly "connectivity". Clearly, such a declaration goes beyond the sorts of statements that are found in the body of international law discussed above. However, as we will see below, a connectivity right is either explicitly or implicitly part of other digital rights frameworks that we analyse.

From the second principle in the list above stems the following;

> *The ability for all to access and contribute information, ideas and knowledge is essential in an inclusive Information Society.*

Here, we see a significant explicit statement of the the importance of "access to information". Whereas the earlier body of international law had to be interpreted as implying a right of access to information/knowledge, the WSIS Geneva declaration states it boldly. However, it is important to note that, like much of the rest of the debate on rights of access to knowledge, the declaration refers to information in the sense of science, technology, and the like; offering no reference to state-held information or any rights that might be associated with that. Still, the expression of the principle is surely significant, and it is but a short and logical step to apply it to government information. As we shall see below, this is a step that several others have taken.

The principle of "capacity building" is also remarkable. It is stated that,

> *Each person should have the opportunity to acquire the necessary skills and knowledge in order to understand, participate actively in, and benefit fully from, the Information Society and the knowledge economy.*

From this, it is easy to infer a duty on the part of the state to provide this "opportunity". Although without explicit reference to the WSIS process, the EUROCITIES charter discussed below appears to follow this line of reasoning.

(1) Burger@Overheid – eCitizen Charter (2005)

A branch of the Dutch public sector ICT implementation organisation, ICTU[133],

> *Burger@Overheid.nl is an independent platform which stimulates the development of eGovernment from the citizen's point of view.*

[133] http://www.ictu.nl/profile.html and http://www.burger.overheid.nl/service_menu/english/who_we_are (accessed 2007/04/07).

It conducts surveys and research into the wishes of the citizenry with respect to eGovernment issues, and acts as an advisor to different branches and levels of government to best achieve their online goals.

In 2005, it launched its “eCitizen Charter”, formulated as a collection of rights (and duties) for citizens in the digital age. The aim was to provide an answer to the question: “What can citizens expect when eGovernment is finally implemented?”[134]. It “is deliberately written form [sic] the citizens' perspective” (Burger@Overheid 2005: 3), and enumerates ten rights that a citizen can expect.[135]

As with the WSIS declaration, privacy and security is explicitly recognised as an important right. But this is actually a relatively small part of the overall charter, being noted only in the “Trust and Reliability” and “Convenient Services” rights.

By far more prevalent is the assertion of rights associated with access to information and access to services. “Transparent Public Sector”, “Comprehensive Rights and Duties”, “Personalised Information”, “Comprehensive Procedures”, and “Accountability and Benchmarking” are all explicitly rights associated with a duty upon government to provide, or make available, information to the citizen. Compared to the WSIS declaration, this set of rights clearly goes much further. This is partly a matter of detail and granularity – the eCitizen Charter is obviously aimed at a different level of the debate to the broader WSIS process – but such a set of information rights over government data nonetheless constitute an extension to those that went before.

In the category of rights to services, we find “Convenient Services”, “Considerate Administration”, and “Involvement and Empowerment”. Again, it is notable how these are rights claims that go beyond the sorts of digital/information citizen rights the preceded the eCitizen Charter. While concerned with privacy, the “Convenient Services” right, as its name suggests, is motivated by efficiency and convenience for the citizen, and thus, in effect, imposes a duty on the state to digitise its services – a duty to engage in eGovernment. The other two rights in this “services” category amount to a duty on the state to be attentive to feedback from the citizenry – on one hand with respect to eGovernment services, and on the other hand with respect to much broader policy-making. The latter is rather an interesting direction. It seems to perceive the increased possibilities for citizen-state communication that come with digital technologies to imply a duty for the state (and citizens) to pursue these new avenues of political participation. While only a small part of the eCitizen Charter, this aspect of the development of DCR forms a more prominent aspect of the other two DCR documents that we discuss below.

Briefly, it is important to note the presence of the “Choice of Channel” right in the charter. While other similar documents emphasise the importance of access to communication technologies and eGovernment services for all, the right asserted here is rather more permissive with respect to the preferences of citizens. In effect, it offers a different solution to the ensuring of equality of access to government than that prominent in other DCR documents: rather than training everyone to use one channel, allow each person to make their own choice of channel. The charter is notably silent on cost implications for a strategy of this sort, however. To the extent that governments services on the web are to be justified on efficiency grounds[136] – and from the Danish embedded case study in this report, this is certainly common – a strategy that requires provision of expensive 'legacy' channels undercuts much of this justification.

Finally, it is interesting to highlight one of the (subsidiary) aims of the charter. That is, to foster greater cooperation and understanding between citizen and state, rather than simply to impose limitations and duties on one side. On the one hand, the “Workbook eCitizen Charter of ...” publication (Burger@Overheid 2005) is formatted as a school exercise book, with each right defined on a page with an explanation of it, followed by space for notes on what “this means for my organisation” and when it is “feasible”. On the other hand, Poelmans (2004: 18) notes that the charter,

---

[134] http://www.burger.overheid.nl/service_menu/english/what_we_do (accessed 2007/04/07).
[135] Please see the Appendix for a full list of the rights listed in the charter.
[136] See also Poelmans (2004: 80), who cites “efficiency” as the first “reason for investments in new ICT applications”.

> *can contribute to the quality of online contacts [...] by reducing unrealistic expectations citizens may have about [eGovernment].*

In this sense, the eCitizen Charter is more a discursive, deliberative document than a simple assertion of well-defined rights. This fits with the voluntary nature of the charter. As noted in the text itself (Burger@Overheid 2005: 5),

> *At present the charter is not mandatory, but is based on the principle: Comply or Explain.*

(2) Tracy Westen – Digital Citizens' Bill of Rights (2006)

The Center for Governmental Studies (CGS) is a California-based think tank that "helps implement innovative approaches to improving social problems and the processes of self-government".[137] Founded in 1983 by Tracy Westen and Robert Stern, it has since then been active on issues related to campaign finance and public interest law. Westen has been active in both government – as a former Deputy Director of the US Federal Trade Commission – and in academia. He currently serves as an Adjunct Professor of Law at the USC-Annenberg School for Communication.

In January 2006, the CGS published a draft of Westen's "Digital Citizens' Bill of Rights".[138] The opening paragraph makes bold assertions:

> *Democratic systems of governance are about to undergo significant, even seismic, changes. These changes will not involve such comparatively simple questions as "Who will be our next President or Prime Minister?" or "Will current political parties retain their control of basic institutions?" The impending changes are more fundamental. They will involve deeper, more structural shifts that will move nations away from their traditional reliance on "representative democracy" toward newer, emerging forms of "direct democracy." The current revolution in communications technologies will play a catalytic role.*

He goes on to claim that,

> *New democratic institutions will alter the rights and responsibilities of citizens as well.*

With this introduction, Westen then sets out,

> *a draft listing of basic principles that might be included in an ultimate "Digital Citizens' Bill of Rights."*

What sorts of rights does Westen assert? His nine types of rights can be usefully split into two groupings. The first amounts to the transposition of existing recognised rights principles into the digital environment – the "digital analogue" of existing rights, one might say. It includes the following:

- "right to privacy"
- "right to assemble"
- "right to freedom of expression"

To reinforce the idea that these are 'old' rights for the new era, all can be traced back to the UDHR and far beyond.[139] In effect, underlying Westen's document is an implicit claim that the online world is simply another arena in which humans interact, and should therefore be subject to the same rights and duties that exist in the physical world. For example, this leads the right to assemble to be transposed to a right to engage in online communities.

---

[137] http://www.cgs.org/about/index.html (accessed 2007/04/04).
[138] Please see the Appendix for a full list of the rights listed in the Bill.
[139] Westen himself cites a number of historical landmarks, including various bills of rights from the United States (and its precursors) going back as far as 1776, and indeed the English Magna Carta of 1215.

As might be expected, Westen's notion of privacy is in keeping with the more modern understanding, such as that found in the CFREU, rather than the older notion found in the UDHR and the like. A right to inspect and correct data held by the state is coupled with a right to stop the state from disseminating private data to third parties. These rights fit closely with those found in Article 8 of the CFREU, although we may discern a greater concern to limit the dissemination of data on Westen's part.

The second group of rights asserted by Westen is characterised by a tendency to impose duties of provision on the state. As defined, the group is composed of the following:

- "right to vote"
- "right to petition"
- "right to information"
- "right to transparency"
- "right to access"
- "right to online services"

Of the list, following T.H. Marshall[140] (Marshall & Bottomore 1991), we might term the first two as "political rights", while the others are more akin to rights of access to information. But these latter rights go beyond mere access. While the right to information is held to include a "Right to access full-texts of all government research online", the right to online services is held to include a "Right to enter into government transactions (e.g., income tax filing) or obtain government services (e.g., auto registration) online". Westen's conception is not merely one of the state being required to open up the information it holds, but one in which the state is required to implement large parts of its traditional activities in an online way. Such an assertion of rights clearly goes some way beyond the existing bodies of law discussed above.

Yet Westen's bill of rights does not stop there. The duties that he seeks to impose on the state go beyond the mere dissemination of existing information and the digitisation of traditional services. He clearly sees the possibilities offered by digital communication as implying an obligation for the state to exploit these new opportunities. Thus, he asserts:

- a "Right to receive free government-supplied e-mail addresses and accounts", and;
- a "Right to participate in periodic, online, non-binding government-initiated public opinion polls, to express opinions on major items pending before local, regional, state and national governments (e.g., government would conduct public opinion polls, post the results, and publicly respond through committee hearings, legislative resolutions, etc.) (alternative to binding ballot initiative)".

It is this aspect of Westen's document – the expansion of the role of the state – that is likely to provoke most dissent. Given existing private provision, it may be argued that it is not clear why there should be a duty on government to supply these services.

(3) EUROCITIES – Charter of Rights of Citizens in the Knowledge Society (2005)

EUROCITIES[141] is a a Brussels-based group that seeks to represent the interests of the "major European cities", primarily to the EU institutions. As a network of 130 cities, it also has an important role as a body that can enhance collaboration and the sharing of ideas between its members. To

[140] See below for a fuller discussion of Marshall's framework and its relationship to the developments discussed here.

[141] http://www.eurocities.org/ (accessed 2007/04/06). Unless otherwise noted, all quotes in this section are taken from this website. Unfortunately, due to its design, it is not possible to provide direct links to sub-pages from which those quotes are taken.

this end, it conducts a number of policy research projects that fall within broad categories of interest.

One such category is the "Knowledge Society", and one project within that is "Charter of Rights of Citizens in the Knowledge Society" – or just the "Charter of eRights" (EUROCITIES 2005).[142] The charter,

> *is conceived as a European blueprint, that aims to be the European model from which local elected governments can draw up their own municipal Charter and determine their own ways of reaching a sustainable Knowledge Society in their local area.*

Of course, signing up to the charter is entirely voluntary, and even having done so, it provides no legally enforceable duties or rights. Even so, by early 2007, EUROCITES reports 39 cities as having signed up to the charter, with a further 18 having "expressed their interest in signing".

Launched in 2005, the charter itself is a short document. It is designed as a leaflet that can easily be carried around, and written in such a way that the signatory of the document is held to have personal responsibilities to pursue and defend the rights set out. For example the declaration that the signatory subscribes to includes the following;

> *I wish to progressively ensure the effective recognition and protection of particular and measurable rights of all citizens in the Knowledge Society needed to overcome any possible threat of the digital divide and to ensure social and territorial cohesion.*

The rights themselves are split into four "chapters"[143]:

- "Rights to Access"
- "Rights to Education and Training"
- "Rights to Online Information"
- "Rights to Online Participation"

"Access", here, is taken to be the combination of Internet access ("preferably via a broadband network") and "security and privacy of any personal data managed through online public services". Neither aspect is distinct to the eRights Charter, although the right to Internet access is only really implicitly present the Burger@Overheid and Westen documents.

The right to online information is composed of a right to the "best quality information produced by public administrations", together with an assurance that disability should not be allowed to preclude such access. As noted above, this kind of "access to information" right does have some support in the existing body of international law.

As with Westen's proposed bill of rights, the eRights Charter goes on to impose duties upon the state – or, in this case, the local government. The education and training chapter asserts a right for "every citizen of the European Union" to be given the opportunity to learn how to use the new information technologies that are now permeating into so many parts of our society. The state is seen as having a duty to provide the necessary training in this regard so that no citizen is unwillingly excluded from the burgeoning "knowledge society". This part of the eRights Charter is distinctive from the Burger@Overheid and Westen documents, neither of which explicitly deals with skills requirements.

The chapter referring to online participation is very similar in spirit to the political rights identified in Westen's Bill of Rights. It seeks to impose a duty on the state to enable a citizen to "participate through ICT platforms in the decision-making processes of his or her local government". Once again, the new possibilities opened up by digital technology can be seen to be harnessed as a tool for more democratic governance.

---

[142] Please see the Appendix for a full list of the rights listed in the charter.
[143] N.B. that "chapter" in the context of this document is akin to an "article" found in declarations like the UDHR, amounting to two or three sentences only.

Having set out the features of the charter, an obvious question is: to what extent has it had an impact on eGovernment in Europe? The voluntary nature of its sign-up process, and the ensuing lack of legal effect even after sign-up might suggest a limited influence. This interpretation would seem to be correct. A personal communication from a person involved with the project indicated an impression that cities are tending to sign up only after they feel themselves to be treating the issues raised in the charter seriously. That is, sign-up is "more like 'reconfirming' their commitment to the development of an inclusive knowledge society".

Civil Society Activity

Having set out the historical context and the more recent developments in the field of digital citizen rights, in this section we provide a brief discussion of the rights issues that appear to be most prominent among civil society organisations (CSOs). In contrast to growing concentration on rights to information and services that we found in the previous section on emerging DCR frameworks, the pattern among CSOs is one of overwhelming focus on issues of privacy and security.

The European Digital Rights organisation (EDRI)[144] was formed in 2002, and is a representative organisation of "25 privacy and civil rights organisations from 16 different countries in Europe". It states that,[145]

> *Members of European Digital Rights have joined forces to defend civil rights in the information society. The need for cooperation among European organizations is increasing as more regulation regarding the Internet, copyright and privacy is originating from the European Union.*

As the description of the membership and the preceding declaration of intent makes clear, privacy is a foundational issue for EDRI. This can be further highlighted by examining the "campaigns" that they are currently engaged in. They are:[146]

- Copyright
- Biometrics
- Data Retention
- Airline Passenger Data

That is, three of the four campaigns can directly be related to concerns of privacy and security.

Taking another organisation, the Open Rights Group (ORG)[147], a similar emphasis emerges. Operating with a UK-focus, and supported by several directors and advisory council members of great prominence in the Internet sector, ORG states its goals as being:

- To raise awareness in the media of digital rights abuses
- To provide a media clearinghouse, connecting journalists with experts and activists
- To preserve and extend traditional civil liberties in the digital world
- To collaborate with other digital rights and related organisations
- To nurture a community of campaigning volunteers, from grassroots activists to technical and legal experts

Its tag line is "Protecting your rights in the digital age". In principle, these goals are commensurate with a broad understanding of digital rights as they relate to the citizen and state. However, analysis

[144] http://www.edri.org/ (accessed 2007/04/07).
[145] http://www.edri.org/about (accessed 2007/04/07).
[146] http://www.edri.org/campaigns (accessed 2007/04/07).
[147] http://www.openrightsgroup.org/ (accessed 2007/04/07).

of the categories under which ORG's weblog postings are made[148], 10 of the 21 substantive topics can be interpreted as being concerned with privacy and security.[149] While the other 11 categories are nearly all directly related to access to information in one form or another, it is notable that none of them are concerned with state-held information, or the duties of the state in relation to it. Taken together, they bear a distinct resemblance to the traditional rights of freedom of expression.[150]

The Open Knowledge Foundation (OKF)[151] might seem to offer some promise as a CSO concerned with access to state-held information, and the provision of eGovernment more generally. Supported by an advisory board composed of, amongst others, several prominent academics[152], the organisation's stated aim is "Protecting and Promoting Open Knowledge in a Digital Age". However, consulting the list of projects in which they are engaged, we find no relation to issues of eGovernment provision.[153]

Despite the preceding discussion, it may be contended that the sample of CSOs discussed here is not representative of the full population of CSOs concerned with the issues under discussion in this case study. Nonetheless, it is remarkable that these leading civil society advocates of "digital rights" that we have identified nearly all ignore the rights issues surrounding access to government information and services. That is, at the very least, we can claim to have found a disjuncture between groups concerned with privacy, security, and freedom of expression, and those concerned with issues around rights to information and eGovernment services. Moreover, we are not the first to note such a divide. Drake & Jørgensen (2006: 5) claim that,

> *the specialized CSOs launched in the 1990s to defend cyber civil liberties have usually stuck to their original mandates, such as freedom of expression and privacy protection, instead of expanding their focus to the broader human rights agenda.*

DCR and Citizenship

What broad patterns can we discern from those elements of the rights discourse associated with eGovernment? As should be clear from the preceding sections, the trend has been one in which issues of privacy, security, and data protection were joined by developing notions of rights of access to information. Initial, and contested, understandings of this right became progressively more recognised by the WSIS and then each of the other subsequent rights documents that we have discussed. But these subsequent documents have then developed the notion of DCR even further. Each, in one way or another, has found it necessary to assert duties on the part of the state to provide services to the citizenry.

Given this pattern of development, we invoke T.H. Marshall's seminal work on citizenship, originally published in 1950. In Citizenship and Social Class, Marshall distinguishes between three types of citizenship: civil, political, and social. He presents a thesis in which these three types developed separately – indeed sequentially, with each tending to lead to the other. First,

> *The civil element is composed of the rights necessary for individual freedom – liberty of the person, freedom of speech, thought and faith, the right to own property and to conclude valid contracts, and the right to justice.*
>
> *[...]*
>
> *By the political element I mean the right to participate in the exercise of political power, as a member of a body invested with political authority or as an elector of the members of such a body.*

---

[148] The ORG weblog appears to be its primary method of communication, so this is arguably a reasonable metric for the concerns of the organisation.
[149] Automatic Vehicle Tracking, Data Protection, Data Retention, DRM, eVoting, Identity, NHS, Police Records, Privacy, Regulation of Investigatory Powers Act, and RFID.
[150] Computer Law, Content Blocking, Copyright, Creative Commons, Intellectual Property, Net Neutrality, Open Source, Public Domain, Release The Music, and Software Patents.
[151] http://www.okfn.org/ (accessed 2007/04/07).
[152] http://www.okfn.org/advisory_board/ (accessed 2007/04/07).
[153] http://www.okfn.org/projects (accessed 2007/04/07).

> *[...]*
>
> *By the social element I mean the whole range from the right to a modicum of economic welfare and security to the right to share to the full in the social heritage and to live the life of a civilised being according to the standards prevailing in the society.*
>
> *(Marshall & Bottomore 1991: 8)*

From this classification, a parallel with the different strands found in the development of DCR can be seen. The early concerns with privacy and security are an obvious analogue to Marshall's civil rights – indeed are an expression of them. They constitute a foundational aspect of what liberty means in the digital era.

While the connection with the "political element" is less obvious at present, a case for it can be made – and it seems inevitable to develop much further in the near future. At one level, the coupling of technology with an emergence of (albeit contested) rights to information has led to increased access to data on political representatives and their activities for citizens. Whether citizen engagement has increased commensurately is another question, but the availability of information has undoubtedly expanded. Less developed, but more relevantly, electronic voting and political participation of other sorts – e.g. see the eConsultation case study in this report – can obviously be mapped onto Marshall's political citizenship.

Finally, it is plain to see an emergent kind of digital social citizenship. Each of the DCR frameworks discussed above had, to varying degrees, aspects that imposed duties on the state to enable citizens to participate in what EUROCITIES termed the "knowledge society". As access to communication technologies – and the government services that accompany them – becomes an ever larger part of what it means to "live the life of a civilised being according to the standards prevailing in the society", this aspect of DCR will surely grow in importance. In Marshall's terms, rights of access to the Internet and its associated technologies appear to set to be foundational. He assesses that,

> *The institutions most closely connected with [social citizenship] are the educational system and the social services.*

In this light, the "rights to education and training" found in the EUROCITIES charter appear particularly well matched.

However, despite seeing similarities with Marshall typology of citizenship, it is relevant to note that the sequence of development that we see for DCR appears to be somewhat different from that discerned by Marshall. While the more civil rights have clearly preceded the others, it has not really been the case that political rights have come before social rights. Instead, the pattern has been one of a simultaneous development of these two elements into the digital context. If anything, social rights are the more developed and recognised, as seen by the widely held concern over the "digital divide".

Furthermore, Marshall's framework does not seem to comfortably fit the developing rights claims to online service provision and eGovernment more generally. Furthermore, to the extent that access to information does not sit easily within Marshall's "political element", this too seems to be partially distinct from the citizenship trio. Perhaps, then, it is possible to start to see the emergence of a fourth aspect to citizenship. One that is based on rights to government transparency, responsiveness, and efficiency – rights to online service provision. While sure to be controversial, it is in this area that digital citizen rights may be most obviously distinct from the past.

At this point, it is worth noting that our analysis of parallels between Marshallian citizenship and the developing digital citizenship is certainly not the only one possible. For example, Bovens (2002) considers a right to government information to be distinct from the civil, political, and social elements of Marshall. Thus, he considers that it is this right that forms a fourth, extended, element. Logically, then, Bovens' conception stops short of identifying a right to service provision. While not positing an extension to Marshall's typology, Moore (1998) also offers an outline of "rights and responsibilities in an information society" that makes explicit reference to Marshall.

Finally, it is interesting to note that the trend has been a development from what can be termed “claim rights” or “rights of non-interference” towards claims of “rights of provision” (Knowles 2001: 140). Our sense is that this trend is set to continue.

Conclusions

To conclude, we have attempted to provide a history of the development of DCR from its ancestors to its present-day young contenders. Up until only about five years ago, the main emphasis has been on what T.H. Marshall called “civil citizenship” rights – those revolving around privacy and security that can be held to lie at the foundation of digital liberty. Given their fundamental importance, it is hardly surprising that civil society organisations have been, and continue to be vigorous advocates in debates around these issues.

As communication technologies and the associated possibilities that they offered for information dissemination and service provision developed, much of the high level policy debate moved on as well. While civil citizenship is largely concerned with limitations on the power of the state, the emergence of digital counterparts to political and social citizenship has been notable for its tendency to try to impose new duties of action on the state. Equality of access to digital communications, and the associated training and skills issues have come to prominence in many contributions to the field recently. It is, therefore, striking that the civil society organisations professing to operate in the area of DCR have largely not adopted this new part of the agenda for themselves. The tendency is clearly for them to continue to operate in the civil citizenship realm.

Finally, the recent DCR frameworks that we analysed are, at least, suggestive of an emerging category of rights claim that is distinct from those discerned by Marshall. This category appears to be comprised of claims of rights to government transparency, information dissemination, and online service provision.

Conceptualising information rights

In the previous section, we identified three strands of digital citizenship: privacy, security and equality of access to digital communications. We also suggested that there is evidence of the development more recently of a fourth strand of digital citizenship; one that is concerned with rights to government transparency, responsiveness, and efficiency. The essence of this fourth strand is a duty on the state to provide digital service.

In this section we develop these strands into a new typology of digital rights. In contrast to Marshall's concentration on “citizenship” as the founding principle for his derivation of categories, the focus in this section is on “information” as the common element. Taking the term “digital” simply to denote an encoding of information, in effect, Marshall's typology can be viewed as drawn from the “C” of DCR, while ours is drawn from the “D”. Despite this differing emphasis, the alternative typology offered here is meant to be purely complementary to Marshall's. Indeed, the issues raised in his Citizenship and Social Class are plainly of a more fundamental nature than those that stem from our typology. Instead, the aim of drawing the distinctions that we do is very much as a useful heuristic for the empirical work that we pursue later in the case study.

An Information Rights Typology

Approaching DCR at the conceptual level, we suggest that DCR can be considered as a body of information rights. Once anything is digitised, it is merely a representation of information that happens to be easily processed. In this sense, when we write about “digital rights” (be they for the “citizen”, or otherwise), we are, in effect, writing about rights over information.

This point leads us directly to a typology of actions that are associated with information. We suggest that a typology of these information actions is the following.

1. Access / Permissions

2. Storage
3. Reuse / Modification
4. Transmission

With each of these actions, it is now possible to conceive of various associated rights. Table 2 sets out a selection of these as they apply in the realm of the citizen-state relationship. The aim is to use the typology of actions to lead us to a set of DCR issues that our case study may examine.

Table 2: A Typology of Information Rights

Information Action	Laws or Claims Relating to DCR
Access / Permissions	Data Protection Rights to information Connectivity and skills for technology use Software requirements Use of non-proprietary data formats Use of software freely available to citizens
Storage	Data Protection Data retention requirements e.g. keeping tax records for a certain period
Reuse / Modification	Correction of state-held information
Transmission	Rights to digital communication with government e.g. email, web, SMS Online services Rights to non-digital communication with government e.g. in person, telephone, letter

Table 2 indicates that Data Protection laws are likely to straddle our conceptual distinction between access and storage rights. They provide limits on both who can access personal information, and what personal information can be stored in the first place.[154]

Finally, legal theorists have distinguished between different "fundamental legal conceptions" that relate to rights (Hohfeld, 1913). Hohfeld termed these:

- No right;
- Duty;
- Right;
- Privilege.

This classification can be seen as a way of assessing the strength of various DCR laws. Thus, for each of the information actions, we may say that citizen-state interactions will be governed by the status that each party has on this scale with respect to the information at issue. A recognisable example of this would be the correspondence between a state's duty to protect personally identifiable information and an individual's right to inspect that which applies to their self. A rather less well known case is in the application of these levels to the sphere of citizen-state communications. Normative and practical questions surround the issue of how each party can expect to communicate with the other[155]. Different jurisdictions have rather different answers to

[154] This issue can be seen, for example, in the accompanying "Eurodac" embedded case – part of the "Public Registries" case study – where restrictions on both what data could be stored in the first place and which agencies would have access to it are noted as important aspects of the case.
[155] These questions flow into the debate around television's "analogue switch-off".

these questions. For example, Denmark has created one of the more concrete rights environments in these respects by giving both administrative units and individuals the right to demand electronic communication – and we discuss this more extensively below.

While we persist with the DCR acronym, it should be clear that "rights" is meant in the broader sense implied by the levels discussed above.

With the typology thus defined, how does it relate to the various historical conceptions of DCR and to the empirical analysis that follows this section? On the former, it is plain that the historical emphasis on privacy and related issues is mostly found within the "access/permissions" category, finding expression in legal rights of privacy for citizens and duties on the state to protect these rights. With the development of digital technologies, data protection laws came to recognise the importance of both the "storage" and the "modification" categories. Limitations – positively asserted conditions of "no right" – came to be imposed on what types of information could be stored in the first place, and rights of access to personal information for individuals became coupled with rights to correct that information where appropriate. In additions, the issues of access to information – both that held by and about the state – discussed in the previous section obviously fall within "access" category in our typology.

The tendency, then, has been for the more established and more recognised DCR issues to fall predominantly within the first three information action categories set out above: access/permissions, storage, and modification. However, in the suggested extension category to Marshall's trio, we may discern a tendency for information transmission rights to be predominant. Rights to the provision of eGovernment services, in the abstract, can be seen as rights on behalf of citizens to communicate electronically with the state. While at one level this may be in the form of simple unstructured emails, the fundamental action taking place is the same when it is in the form of highly structured and controlled transactional eGovernment services. The previous section, then, suggests that future developments in DCR may be concentrated in the area of transmission rights to a much greater extent than we have seen up to now. We should probably expect to see more claims associated with what McIver et al (2003) term a "right to communicate".

Empirical Application

As we have seen, the concept of human and citizen rights, even when limited to the digital realm, can be extremely expansive. More general (and sometimes contested) normative rights common to liberal democracies can have a wide range of implications as societies begin to operate more and more in an "online" way. These broader rights issues are not even limited to the citizen-state relationship. Rights claims revolving around protections of, say, "digital property" may also be asserted. Debates in this non-citizen-state area influence the actions of governments in more regulatory ways. That is, they will tend to lead to legislative action rather than impinge on the administrative activities of the state.

While recognising these broader societal rights issues, our empirical approach takes a somewhat narrower view. We concern ourselves only with how rights issues relate to the provision of eGovernment services. The evolving area of citizen rights may require legislative action from government in order to give statutory force to normative principles, but this lies within scope for our study only to the extent that these normative principles and/or legislation are found to have a discernible impact on eGovernment provision. Our concern is therefore in the area of what political scientists term public administration.

Forming part of the broader Breaking Barriers to eGovernment project, the approach that pursue focuses on the extent to which DCR affects both the ways in which, and the extent to which, eGovernment services are provided. In this way, DCR is conceived of as an intermediary factor that can either inhibit or enable eGovernment projects. For example, rights of privacy that are often given statutory force through "data protection" acts may form a barrier to the sharing of personal information across government departments. They may also act as an enabler to take-up of eGovernment services as citizens have more confidence that any personal information that they supply will not be used inappropriately. Similarly, legally enforceable rights to communicate with the state through electronic means are also likely to act as a boost to the provision of eGovernment

services as branches of government become required to invest in their IT infrastructure to service those rights.

An approach of this sort may not limit itself to those rights that are legally enforceable or recognised, however. Political theorists have found it possible to distinguish between “moral” rights and “legal” rights.[156] While this kind of legal positivism that perceives the law itself as devoid of moral content is highly contested, it nonetheless lends weight to the idea that some rights claims will have found legislative or judicial support, while others will not. However, it remains an empirical question as to whether this distinction is important in practice. The effect of legally enforceable rights and duties may not be very large if they are of limited practical importance to citizens or the state. By contrast, widely-held normative values that imply rights and duties, but have no legal recognition, could very well be an important factor affecting the decisions of policy-makers and eGovernment implementers.

Relevant normative concerns are not difficult to think of. Issues such as the “digital divide” are grounded in normative concerns over equity. If societies harbour notions of rights to equal treatment, then provision of eGovernment services that are empowering only to those with Internet access or large amounts of skill and experience in the digital realm are likely to be controversial and contested. Concerns over equity may lead to the requirement that the provision of enhancement of digital services be coupled with investments in the upgrading of more traditional modes of contact – e.g. telephone call centres and over-the-counter interactions at post offices and the like. In this way, amorphous notions of a right to equitable treatment may have important implications for eGovernment provision.

[156] c.f. Dworkin (2005: Chapter 7)

Case Study: Denmark

Tim Hicks

Oxford Internet Institute, University of Oxford

In this embedded case study, we present the results of field research into the DCR issues surrounding prominent eGovernment projects in Denmark. During a three day visit to Copenhagen, we conducted interviews with a number of civil servants and civil society representatives. We sought to investigate the impact that Digital Citizen Rights (DCR) issues have had on the extent, implementation, and take-up of eGovernment in Denmark. Applying the conceptual framework set out above, we use the evidence that we gathered to show how the Danes have ignored, approached, or (often) answered the questions that arise regarding the relationship between information, citizens, and the state. In doing so, one of our aims was to uncover the extent to which DCR has been integral both explicitly and implicitly to eGovernment strategies in Denmark, and thus the extent to which it may be seen as an important underpinning for successful eGovernment. While our findings are obviously applicable to Denmark specifically, the aim is to draw implications for the broader European context.

Denmark was chosen as an embedded case because initial research suggested that (at least some) DCR issues have been explicitly addressed. The "eDays" of September 1st 2003 and February 1st 2005 (discussed more fully below) represent unusually overt governmental attention to the rights issues around electronic transmission of information – culminating in numerous legislative changes[157]. The Danish government, in pursuing its "modernising" agenda, has also appeared to acknowledge rights associated with data sharing as a necessary consideration in how to structure new eGovernment programmes[158]. Thus Denmark provides an example of the application of the higher levels of Hohfield's 'scale' of rights discussed above.

In keeping with the approach set out above, our research aimed to draw out the ways in which DCR issues – which we defined using the theoretical framework developed earlier – have impacted upon the provision of eGovernment programmes. The particular focus of our research was into the evolution of the central citizens' portal(s) – now named borger.dk, but taking various guises in the past. The portal has been through various incarnations over a period of at least 10 years. Originally designed as a purely static information service – what might be termed "Web 1.0" – there have been efforts to increase the interactive and personalised elements of the site. These efforts continue, and even as the newest version of borger.dk was launched in January 2007, a new version that aims to be a platform for individualised services was (and is) actively being planned.

Based on the availability of sources, we concentrate on just two iterations of the borger.dk project. The first, which went "live" in January 2007 was produced by one of the two main eGovernment agencies in Denmark (the ITST[159]), while the second is currently in the planning stages, and is under the auspices of the other main agency (the Digital Taskforce).

Specifically, our interest in borger.dk revolved around issues of "access" to information. Before embarking on the field research, our expectations were that the most relevant issues would be those around data protection and privacy on the one hand, and the duty to make publicly-held information available to citizens on the other. During the field research, we also took the opportunity to learn more about the impact that the eDays have had on the eGovernment landscape in

---

[157] In 2002, there were 88 amendments to 21 laws with the aim "to remove the legal obstacles to digital communication". http://www.e.gov.dk/english/results/2002/the_removal_of_legal_requirements/ (accessed 2007/02/17)

[158] "New technology must contribute to the creation of increased collaboration across the boundaries of the public sector. With regard to the legal rights of citizens, it must be ensured that the exchange of information is possible between state IT systems, so that people come to experience the public sector as a well-functioning whole." (Government of Denmark 2002: 21)

[159] See below.

Denmark. Our goal was to discover the extent to which these obvious digital citizen rights reforms have influenced the plans and achievements of those concerned with online government service provision. While eDays may reasonably be expected to have had an impact on the design of borger.dk, any effect that they have should go far beyond citizen portals.

Before setting out the findings of our research, the next section provides some institutional context for the Danish eGovernment actors. The section following that sets out a more detailed description of the various reforms and projects that the study focuses on. With the context for the case study thus set out, we finally move on to a discussion of the interaction between DCR and eGovernment in Denmark.

Institutional Context

The institutional context in which eGovernment projects are directed and implemented, even purely at the central government level was described as "typical[ly] Danish... the relationships [between different agencies] are very messy". Despite this – or perhaps because of it – the division of concerns between the two main central government agencies concerned with eGovernment appeared to be clear to all concerned.

IT- og Telestyrelsen (ITST)

The ITST (the National IT and Telecom Agency) is an agency under the auspices of the Ministry for Science, Technology, & Innovation. It asserts that its[160],

> *principal task is to develop and implement initiatives within key areas of the Government's IT policy strategy. A strategy that aims to ensure an optimal framework for IT and telecommunications and conditions that will enable citizens, businesses and the public sector to realize the network society.*

Involved in numerous eGovernment projects, the primary interest we had in the ITST was its input into the various centrally organised portals in Denmark (which are further discussed below). While not actually directly implementing projects itself – i.e. all software development is outsourced to contractors – the ITST is the closest of the state agencies to the technical end of the development process. A team of 36 ITST employees was tasked with implementing the first generation borger.dk portal (again, discussed below), although this was augmented by a small development team and call centre staff.

Digital Taskforce

Closely related to the operations of the ITST is the Digital Taskforce. This 20-strong group is located across town at the heart of government in the Ministry of Finance. Its,

> *task is coordinating cross-government IT policy, not on the technical stuff but on the more policy stuff, and running cross-government projects like borger.dk. (Interview 2)*

Commensurate with this purpose, it is a truly cross-government agency with staff seconded to it for periods of up to around two years. Those staff are drawn from the Ministry of Finance itself, from other central government ministries and agencies (including the ITST), from the regions, and from the municipalities – including their association, KL. This structure is intended to allow the Taskforce to operate both "cross-government and also cross-government-levels", which seems likely to be a response to the strongly decentralised nature of the Danish state.

Like the ITST, the Digital Taskforce has been involved in numerous eGovernment projects since its inception. These have ranged from the production of common IT-related contracts, to the design of versions of the borger.dk portal, to mass media marketing campaigns to publicise the availability of

[160] http://itst.dk/wimpdoc.asp?page=tema&objno=95024027 (accessed 2007/03/06)

eGovernment services.[161] For the purposes of the research for this case study, our main interests in the Digital Taskforce stemmed from its leading role in both the second (under development) borger.dk portal, and the various eDays.

Kommunernes Landsforening (KL)

Denmark has a long history of a highly decentralised state. Until 1970, local government consisted of "86 boroughs and approx[imately] 1300 parishes within 25 county council districts" (Ministry of Interior & Health 2006 : 5). In 1970, with the intention of increasing the size of local government units so that they were better able to benefit from economies of scale in service provision, "the number of counties was reduced to 14 and the number of municipalities to 275" (Ministry of Interior & Health 2006: 6). Decentralisation of service provision continued after the 1970 reform, and the degree of discretion available to local governments was further enhanced by the introduction of block grants rather than earmarked funding from central government. Finally, in January 2007, a further reorganisation of local government was completed. Based on a similar logic to the 1970 reform, the new structure is one of 98 municipalities and five regions – counties are abolished. Despite these reforms, local government retains its important role in the provision of the welfare state, including health care and education. The point being, local government is at the heart of the Danish state, and therefore vital to numerous eGovernment programmes.

Partly as a result of these recent reforms, the KL is an evolving institution that acts as the representative association for the municipalities. Membership is voluntary for each municipality, and those who join pay a fee to do so, but central government also provides KL with funds. As the principal agent representing the views of municipalities, KL has been closely involved in many centrally run eGovernment projects, not least the two borger.dk and the eDay projects under consideration here.

eGovernment Projects

In this section, we provide a little background information on each of the eGovernment projects that we focussed on during our field research. The aim being to make the issues discussed in the following section regarding the impact of DCR on those projects more comprehensible.

The borger.dk Portal

First Generation

Development of the first generation portal involved the joining together of "two large websites". One (danmark.dk) "was mostly a state [central] government portal [...] which was quite strong on information". The other was a more "self-service" oriented portal "made mostly by the municipalities and their organisation". In this way, this first generation portal is something of a hybrid in that it offers relatively large amounts of static information, together with some facilities for online transactions. The functionality is such that,

> *you can choose your municipality, and you will be shown the services that you can use [based on that location]. (Interview 1)*

Underlying this portal is an information architecture that is expected to survive into the second generation portal. This structure is one in which the various pieces of functionality are componentised, and joined together by standardised interfaces. This allows different organisations – such as ministries, municipalities, and even private sector actors[162] – to produce different services

[161] A selection of projects can be found at http://www.e.gov.dk/english/egov_projects/index.html (accessed 2007/03/17).
[162] The inclusion of private sector actors into the portal is currently not possible only on policy, not technical, grounds. However, it is being actively explored by the government and appears to be viewed very positively (Interview 1).

as pluggable components for the portal. Furthermore, they can do so based on the availability of common tools, such as “single sign-on” (i.e. authentication). The role of the ITST group is, then, to define the standard interfaces and common tools that service providers can use.

> *We don't make the services ... We make the overview, we make the methods... kind of a toolbox to make good services, but we don't make the services. (Interview 1)*

In terms of project oversight and resources, the ITST team implementing this first borger.dk was supervised by an eight member board comprised of civil service representatives from central and local government[163]. The board was chaired by a Director from KL, and financing for the project came from ITST and KL.

Second Generation

As noted above, even while the first generation borger.dk was being prepared for launch, a second generation portal was already in the planning stages. The aim of this second generation borger.dk portal is to more fully unite the services that are, and will be, offered by all levels of government. To this end, the portal will be restructured so that the information and service options that you are presented with are far more personalised than is currently the case. Where citizens now select their municipality and are then presented with relevant information for their area, the second generation portal will, after logging in, present the citizen with options that relate specifically to their own (perceived) needs and interests. Services will be channelled through a number of “themes”, such as “My Home”, “My Kids”, and “My Economy”. Transactional services of the sort that appear in these themes will be at the heart of the portal, which will therefore go very much beyond being a simple information dissemination tool.

The second generation portal is scheduled for launch in the “first quarter of 2008”, but there exist plans stretching further into the future. Central government has declared a roadmap for “all kinds of public agencies” to put services on borger.dk, so that in 2008 “they can do it, in 2010 they should do it, and in 2012 there's no way back – you have to do it”.

In a noteworthy change, the supervisory board for the second generation borger.dk portal only has municipality representation through KL. One interviewee noted that they felt the change was stemmed from KL wanting to be the single point of representation for municipalities, and that the board structure for the first portal was rather unwieldy - making it “one of the barriers” that were experienced. This view was corroborated by another interviewee.

The eDays

eDays 1 and 2

In the area of DCR as it applies to information transmission, Denmark may be considered to be a leader. September 1st 2003 was declared by the government to be “eDay” in Denmark. After that date,[164]

> *all Danish state, regional and local government authorities have a general right to demand that communication with other authorities be exchanged electronically, and thus the right to refuse paper-based communication.*
>
> *In this initial formulation, the right to digital communications was limited to “non-sensitive” information.*

However, from February 1st 2005,[165]

---

[163] But not the regions (Interview 1) – presumably the only reason being that they were not in existence when the first generation *borger.dk* portal was being developed.
[164] http://www.e.gov.dk/english/egov_projects/eday2/eday/index.html (accessed 2007/04/09)
[165] http://www.e.gov.dk/english/egov_projects/eday2/index.html (accessed 2007/04/09)

> *eDay2 took this general right an important step further - even sensitive communication had to be exchanged electronically. The goal was for 40% of current letter post to be replaced by electronic post by November 2005.*

Further, it was claimed that,[166]

> *eDay2 will not only bring benefits to the public sector; as a key initiative in realising the Danish vision for eGovernment eDay2 will also mean that citizens and businesses will be given the right to communicate electronically with the central public authorities, using digital signatures. They will as far as possible also receive electronic replies, if they so request.*

The assertion of rights in this area is clearly meant to have an impact on government efficiency. In fact, the Danish government estimated that eDay 1, alone, would "generate savings of about €25 million a year in stamps and more efficient workflows for mail handling"[167].

In discussion on the two eDays, the Ministry of Finance source indicated that their significance had only really been felt within the state – albeit at all levels: from municipality, to county, to central government. That was obviously the case for eDay 1, which limited electronic communication rights only to those documents that did not have privacy implications for individuals – i.e. documents that identified individuals in any way. This limitation precluded citizens from using the right established in eDay 1 as any electronic communication from them to a branch of the state would inevitably reveal their identity.

While eDay 2 removed this restriction, thus giving citizens the right to communicate with the state in electronic form, again it was felt that the effects of the reform were almost exclusively felt by the various branches of the state, and not directly by citizens. The state has become far more likely to exchange data internally in electronic form, and there is a perception of increased efficiency as a result. However, the requirement that citizens utilise digital signatures[168] for all communications with the state was felt to be, currently, too large an impediment to take-up of the right established by eDay 2. Lack of usability for such signatures meant that for most citizens, email exchanges with the state were not really possible. Even for those who could be deemed capable of using email with the current technical solutions, a further problem appears to be relevant.

> *Because, I think, one of the very big problems is that the councils are very, very, bad at [responding by email] [...] You can wait up to two weeks [for an email response]. [...] When you call, you get the answer right then. (Interview 4)*

In one large municipality, it was said that only about 1% of citizens were using email to communicate with their local government. The respondent felt that this was the result of a combination of bad organisation and rejection of email as an efficient channel that stops use of email by municipalities.

By contrast, the use of authenticated email communication using digital signatures within the state was held to be very prevalent – possibly as a result of specific training that can be afforded to users in this environment.

eDay 3?

Recognising that more user-friendly services will be needed in order to draw the citizenry into greater reliance on electronic communication with the state, those involved with the second generation borger.dk portal suggested that a third eDay – "eDay 3" – was likely, perhaps even within the next two years. Still in the formative stages, it is felt that such a reform would have to couple an improved webmail-like service that provided a more comfortable user-interface to the secure signature functionality, together with some form of more strongly-articulated citizen right to

---

[166] ibid.
[167] http://www.e.gov.dk/english/egov_projects/eday2/eday/index.html (accessed 2007/04/09)
[168] Which are themselves provided by a government project: c.f. http://www.egov-goodpractice.org/gpd_details.php?&gpdid=1786 (accessed 2007/03/06).

electronic communication with the state. Unfortunately, no further information as to the latter is currently available.

The Impact of DCR on eGovernment Projects

With a clearer picture of the relevant eGovernment projects, and the institutional context in which they operate, we now move to the substantive discussion of the ways in which DCR issues have affected the those projects. The discussion initially centres around the two most prominent rights issues to emerge from our research: data protection and privacy on the one hand, and 'rights to information' on the other. We then turn to a more general discussion of some of the other issues that stood out.

Access: Data Protection and Privacy

> *When we talk about citizen digital services and the Danish ICT policy, privacy is probably the one core right that is challenged. (Interview 3)*

Perhaps unsurprisingly, issues surrounding data protection and privacy were found to be easily the most prominent in the thoughts of eGovernment implementers and civil society groups, alike. While several interviewees expressed puzzlement and intrigue at what we could be referring to when speaking of “digital citizen rights”, their responses to questions quickly turned to data protection laws and the normative value of privacy.

With respect to borger.dk, the chosen architecture has important implications both from an implementation and a rights perspectives. Potentially, then, this could be an area in which DCR, in the form of data protection and privacy, imposes difficulties on the provision of eGovernment services. However, the interviewees, with only minor disagreements, were quick to assert very little in the way of a conflict of this sort. The reasoning of the civil servants was that the chosen architecture is optimal from both implementation and data protection perspectives.

In the first case, it removes the need for a single agency to implement and provide all online services and thus removes a potential bottleneck in the roll-out of new services. Not only that, it allows for better services to be developed as the particular agencies, ministries, municipalities who have direct expertise with the policy area are the ones that implement the portal service/component. With respect to data protection and privacy, the architecture makes it possible for the databases underlying each service/component to be independent of all others, thus limiting the possibilities for data sharing across previously separated parts of the state. In essence, this reasoning amounts to a claim that the portal project will not necessarily act as a driver for ever greater data integration.

So, although the presence of data protection legislation meant that the chosen architecture was effectively required by law, the civil servants felt that “it was also the most appropriate one”. While this was the broad impression given by most respondents, one interviewee did express some frustration at the perceived restrictions of compliance with data protection laws. Referring to government legal advisers involved in the eGovernment policy process, the interviewee noted that, “Sometimes, I think, they stop some innovation”.

As might be expected, the civil society rights representative that we interviewed had a somewhat less positive view regarding the prospects for privacy in the developing Danish eGovernment environment. Unfortunately, full details of the portal architecture had yet to be revealed to non-governmental organisations (NGOs).[169] Still, it is fair to conclude from the views expressed to us that there remains some distance between the civil servants and rights groups over the steps necessary to guarantee privacy. As one civil servant remarked,

> *We think that we have a schism between what the Danish citizens want... They want joined-up services - 'Just bring it together and show it to me!'. And then we have some privacy professionals who are very much worried, but it's not the citizens. The citizens*

[169] Consultation on the issues is due to happen in the next few months (Interview 2).

> *trust that we use their data in a proper way and insist that we use it for delivering more timely services.(Interview 2)*

Perhaps inevitably, this differing emphasis on privacy leads advocates of the latter to propose different technical solutions to eGovernment services, as the following quote from the civil society representative makes plain.

> *There is a core conflict, definitely, but I think it's also often emphasised maybe too much. So you get the feeling that you have to choose basically between convenience and privacy. A lot of the more technical people I know that, for instance are involved with privacy-enhancing technology, would argue that that debate is wrong from the very premise of it... that it doesn't have to be either or. But that would imply rethinking solutions in a more radical way on the technical level. (Interview 3)*

It was suggested that one solution that might emerge from such a "rethinking" is that of "pseudonymity", whereby citizens utilise different unique identifiers when interacting with different parts of the state. This provides greater protection against the state 'joining the dots' between the transactions of an individual.

Despite the differences of opinion regarding privacy, there was near unanimity from both camps on the question of whether data protection and privacy impose a barrier to eGovernment. While they often impose requirements on the design and implementation of online services, these requirements are not felt to be problematic to fulfil.

Access: Rights to Information

The bearing of issues revolving around 'rights to information' appear to have had relatively little bearing on the recent development of eGovernment in Denmark. Not only is this true from the perspective of both civil servants and civil society organisations, but the view was expressed that there had actually been a reversal away from that kind of thinking in the past five years, or so. The following quote makes this plain.

> *With the borger.dk project, we are aiming to give the citizens a right to data. We are aiming to give them access to data. But not as much in a rights-based thinking – that you have a 'right' to see the data, and then you have some long list. [...] More in an empowerment-influenced thinking. We will give you the data that enables you to act to improve your own situation. And what is important is that we give data that is relevant to you and can help you in your situation. It is not so much an ambition to give you 100% [of the] data. So they [the previous rights-oriented projects within the Digital Taskforce] are both an inspiration, but also we have moved away from the rights aspect and more engage in an empowerment thinking. (Interview 2)*

That quote is very revealing. Previous concerns with abstract rights were seen to have led to a dead-end in which services and procedures were developed, but met with no public demand. Despite the claim that "we are aiming to give the citizens a right to data", it is clear that doing so is to a very large extent simply instrumental to achieving higher take-up of eGovernment services by the public.

More specifically, the idea of 'rights to information' seems to have had very little influence, if any at all, on the types of information and services that are either currently or planned to be available via borger.dk. With respect to the "themes" for the second generation,

> *The ones that we have chosen now as the first four... that is quite coincidental. What departments are ready... have good projects that we could integrate... have been positive. (Interview 2)*

To that list was also added the idea of high impact services that are in great demand by citizens. So,

> *From the outset we knew we had to get the tax department, because that is so big in digital government.(Inteview 2)*

This kind of viewpoint – one of pragmatism rather than rights – was , to some extent, expected of the civil servants. The views of civil society in this area were, however, less predictable a priori. Our research revealed, in the first instance, little concern for these issues from a leading rights organisation as well. Speaking of the first generation borger.dk, the interviewee commented,

> *I must say, I haven't really looked at the one that was just launched. I haven't really used it. [...] It hasn't really been present in my mind. (Interview 3)*

However, this absence of concern for the information and service content of the portal was only applicable in the limited area of whether citizens could be seen to have a right to find certain information on the site. Further questions yielded noteworthy concerns about the extent to which the provision of eGovernment services would effectively exclude members of the Danish public. That exclusion could be the result of lack of Internet access, lack of technical skills, lack of language skills, or physical disability. In this sense, rights conceivably offer a normative barrier to eGovernment. A right of equal access to information for all citizens imposes higher accessibility requirements for online services. Implicitly, at least, this issue was recognised by some of the civil servants.

> *This [the portal] is a supplement. There is a 'canal strategy', I think we call it. A strategy where there's the phone, there's email, there's e-dialogue, [...] there's the personal – the possibility to go personally to the office – and there's this one [the portal]. But of course, it is an aim for the public sector to move some of those who actually want to do the things on the Internet [onto that channel]. But there's [sic] still all the other [channels ...] available. (Interview 1)*

Further,

> *When we are making this citizen-centric focus [portal], we are aware[170] that there are, of course, a part [sic] of the Danish population who will never use the Internet. And actually, they use a lot of public services, but they won't be able to access this [portal].(Interview 1)*

Despite this stated strategy, there is some movement towards compulsion in the area of eGovernment. The unemployed are required to provide an electronic CV as a condition for receiving benefits, and there are moves to make certain aspects of university student finance entirely online.

The final 'right to information' point worth making is that, by virtue of its very decentralised structure, Denmark is potentially very susceptible to claims of “postcode lottery”, whereby different citizens receive different services simply by virtue of where they live. The interviews revealed that this is, indeed, the case as there are “very big” differences in the availability of eGovernment services across municipalities.

For two related reasons, this seems set to continue. First, central government bureaucrats appear very wary of taking on responsibility for more direct service provision.

> *The responsibility to make digital services is still locally placed. We find it to be a very bad idea for us to overtake [sic] that responsibility. (Interview 1)*

Our impression is that this is due to a perceived benefit of a division of labour in which the centre provides core tools, and local government provides (most of) the actual services for the citizen with these tools.

Second,

> *The councils are also afraid of too much [sic] [central] government decisions, because they think, and I also think, that the local government is very good [at making] new things and realis[ing] a need in the community or for the citizens [...] If you make a portal where everything has to be decided from the top, it will be very difficult to make new solutions from day to day.(Interview 4)*

---

[170] “Approximately, I think, 8 percent of the Danish population is conceived to be totally out of reach digitally. And there is, actually quite new analysis, which says there is about 40 percent of the Danish population has quite poor skills [...], which is mostly elderly.” (Interview 1)

It appears, then, that the Danes are comfortable with trading some extra innovation and customisation for a little less equity and uniformity.

Further Discussion: Efficiency

Common to all respondents was the view that the drive for greater efficiency is an extremely important driver for just about all eGovernment programmes. One might see this as being the primary motivation on the 'supply side'. On the 'demand side', we inevitably find the expectations of citizens.

> *There are, I think, two things [...] There are fewer and fewer young people, and more and more retiring, so you need to be more efficient [...] But the other thing is also to, I think maybe, accommodate the expectations in the Danish population that of course it should be possible to sign up your child for daycare through some kind of digital service, and so forth. (Interview 1)*

The drive for efficiency necessarily creates a drive to increase take-up of service provision so as to maximise the returns to the eGovernment investment.

> *We have very big unrealised, ungained, potential for efficiencies if more citizens use our applications. (Interview 2)*

Our impression from all interviews was the efficiency agenda was highly pervasive. In effect, with the partial exception of data protection and privacy, rights issues were incidental to eGovernment actors. That is, where rights-based policies were employed – most notably for each of the eDays – they were mainly aimed at increasing take-up of digital services by forcing particular actors to respond to the wishes of early adopting citizens.

Rights can be seen as incidental in another sense as well. One civil servant implicitly suggested that there were democracy-enhancing possibilities for the eGovernment agenda.

> *We hope to engage the citizens in the public welfare more. And we see that we can use the digital opportunities to do this. (Interview 2)*

However, this appeared to be a held to be a secondary benefit. That view is certainly shared by the civil society interviewee, who commented that,

> *the political rhetoric, as I read it, around eGovernment is so focussed on efficiency, more than these democratic aspects of getting the citizen different means to participate, or better means, or using it to create a different kind of interaction between state and citizen... creating new spaces for that meeting. It's very much an effectiveness agenda. (Interview 3)*

In many respects, this differing emphasis on the potential benefits of eGovernment provision parallels an earlier debate in Denmark over 'citizen cards'. Hoff and Rosenkrands (2000) highlight two competing strategies regarding the purpose and design of those cards in the mid-1990s: one “efficiency-oriented” and the other “citizen-oriented”.

In keeping with this idea of competing strategies, the civil society interviewee also felt that the efficiency agenda was even dominant over the privacy agenda.

> *For instance, if you take the Digital Taskforce, they haven't focussed on this [privacy] very much. They are completely on the line of effectiveness – all the stuff that you can do with technology and how you can exchange... And then privacy considerations would be more like an appendix at the end saying 'yeah, by the way, we have to, of course comply with Danish data protection legislation. But they wouldn't so much think it up front as a core issue, because there would be an assumption that [...] it's not really a problem in Denmark... the government [are] good guys. (Interview 3)*

This final remark was echoed more than once, and in multiple interviews. “Trust” seems to be held as an important aspect of the Danish attitude towards eGovernment. To the extent that it is true that the Digital Taskforce, along with other state actors in the eGovernment policy realm, see privacy as

a low priority, this may very well be a reflection of the underlying ambivalence of the citizenry to the issue.

> *Denmark [... is] different from many other European countries in that the Danish citizens have very high trust in the government and in Danish authorities (Interview 2)*

Broader Barriers to eGovernment

The Seven Barrier Categories

The Breaking Barriers Project, funded by the EC, identified and explored the key barriers to eGovernment in Europe. The project team proposed seven key barrier categories of obstacles to eGovernment progression. The categories are intentionally broad and tied to a multitude of more specific barriers relevant at different governance, institutional and jurisdictional levels. This categorization is particularly valuable when discussing the barriers relevant to this case which may have relevance for other eGovernment initiatives. In summary the barriers are: leadership failures, financial inhibitors, digital divides and choices, poor coordination, workplace and organizational inflexibility, lack of trust and poor technical design[171].

While not directly related to DCR, this case falling within the broader Breaking Barriers to eGovernment project makes it appropriate to deal with the specific barrier categories that have been found during the broader research project. In this section, we briefly describe the applicability of each category to the Danish borger.dk project.

Leadership failures: We found little to suggest that leadership failures were relevant to the Danish portal project. One respondent suggested that many of the ideas that are currently being implemented were being considered as early as the mid-1990s, and suggested a lack of will to pursue them at that time. However, it should be emphasised that this was but one view among several.

Financial inhibitors: None of the interviewees made any reference to financial inhibitors. Indeed, one of the primary justifications for the project was to achieve efficiency savings.

Digital divides & choices: We found some evidence to suggest that digital divides and extending access to digital services may be something of a barrier. However, its path of effect was slightly indirect. That is, the need to maintain more traditional channels or to provide training and assistance to sections of the population imposed increased costs on the project rather than precluding specific provisions.

Poor coordination: There was some evidence to suggest that coordination among the various state actors has posed problems. The adjusted structure of the new borger.dk project board – excluding municipalities from direct representation and using KL to provide this instead – was held to be a response to earlier difficulties in decision-making. The larger project board that operated previously was felt to be somewhat unwieldy.

Workplace and organizational inflexibility: We found no evidence of this barrier category being important. However, it should be noted that our research design was not aimed at detecting it. Our interviews concentrated on those agencies that were involved in the architecture of eGovernment services. The more likely venues for this barrier to be felt would be in departments and agencies that utilise this architecture to implement electronic versions of services that they already provide.

Lack of trust: Civil servants and civil society actors, alike, held that lack of trust was not a major problem. On the contrary, several interviewees noted that Danish citizens have distinctively high levels of trust in their state.

Poor technical design: We found no evidence to suggest that poor technical design has been a barrier.

---

[171] For more details about the Breaking Barriers to eGovernment project please see http://www.egovbarriers.org

Conclusions from the embedded case

What conclusions can we draw from this case study on the interaction between DCR and eGovernment provision?

One of the clearest things to emerge from our research is that data protection and privacy are the most oft cited DCR issues surrounding eGovernment. Although potentially a constraint on service provision and design, nearly all interviewees expressed the view that it would be wrong to characterise privacy as a barrier to eGovernment per se. While views on what would constitute best practice for the design of the state information architecture differ between state and non-state actors, resolution of those differences would likely leave privacy issues as a relatively minor considerations for future eGovernment projects. Until that time, privacy will probably remain a rather contested issue in the policy process.

Another clear conclusion is that the notion of eGovernment service provision being driven by a perceived 'right to information' is wide of the mark. We found no evidence that normative values were applied over decisions about which sorts of information or services to provide to citizens. Efficiency, and by extension, pursuit of take-up, were by far the most important justifications expressed for the development of services.

Following on from that finding, it also appears to be the case that the prominent 'transmission rights' that have been asserted and proposed in Denmark (i.e. the eDays) are largely seen as instrumental to increasing take-up of digital interaction with the state. In that sense, the eDays are, in the main, simply policy tools to increase state efficiency, rather than rights with particularly normative underpinnings.

The very fact that digital rights have been used in Denmark to increase take-up and provision is evidence to the idea that DCR can be seen to have positive impacts on eGovernment. In sum, we have found that the most prominent DCR issue (privacy) need provide very little in the way of a barrier to eGovernment. Meanwhile, other rights policies can and are seen as positive enablers.

Conclusions

So, following the analysis in each of the sections above, what broad conclusions can we draw regarding the relationship between digital citizen rights and eGovernment? In this final section, we draw together the findings from above and highlight what should be considered the most relevant from a policy-maker's perspective.

DCR Development

In the section on historical and recent developments in DCR statements, a number of conclusions stand out. At the most basic, DCR is very clearly an emerging field. This is true in two senses. While concerns over individual privacy and security are hardly new – being widely acknowledged in the context of human rights – it is fair to say that governments and societies are still contending with what implications these established principles have in the digital era. Technological advances have, in effect, removed some of the historically unspoken barriers to state intrusion into the more private parts of citizens' lives. In this light, it is unsurprising that we find a concentration by civil society organisations active in the field of digital rights on privacy, security, and the like. The core of claims made in this area are over rights of non-interference – of limitations on the state.

But despite the prominence of disputes, this part of DCR is actually very much the more developed. Following EU action, data protection legislation is now in place right across the member states. Limitations on the access to and storage of data have legal force. Individuals have rights to inspect and correct the data held about them. Seen through T.H. Marshall's citizenship lens, the relative strength of this aspect of DCR seems logical. Marshall showed that “civil citizenship” – “the rights necessary for individual freedom” (Marshall & Bottomore 1991: 8) – was the first of three elements

of citizenship to develop. Taking privacy to be foundational for “individual freedom” in the digital age, its early development seems apt.

While these issues of civil digital citizenship are widely acknowledged, we have found that there are other nascent aspects to DCR that are both less well understood, and less well recognised. Recent attempts to codify these emerging aspects have met with mixed receptions and made only limited impacts on policy and service provision. These newer statements appear to be largely concerned with staking out the territory, and can be characterised as aspirant rather than applied practice.

Although in the early stages of development, these newer categories of DCR seem set to be the most prominent moving forward. In contrast to those rights that are associated with civil citizenship, a distinguishing feature of these emerging categories is that they are composed of claims of rights to provision – of duties on the state to provide information and services through digital channels. Coupled with these are claims of rights to connectivity and the skills that amount to prerequisites for its use. In our view, it is these areas that current developments in DCR that most clearly move beyond Marshall's three-part typology of citizenship. Thus, it is in the sphere of rights over information transmission that we see scope for an emergent fourth part to the Marshallian scheme.

DCR Influences on eGovernment – Empirical Evidence

In many respects, our empirical research in Denmark reinforces the findings from other sections. In accordance with the prevalence of privacy and security in historical debates and current civil society discourse, civil service eGovernment implementers overwhelmingly referred to the same issues when questioned about what aspects of DCR were most relevant to them. Given the nature of these issues – as limitations on the actions of the state – it might be reasonable to expect that DCR, as currently experienced, provides only barriers to eGovernment.

The surprising truth, however, seems to be that individual privacy is not held to be a barrier. Strong disagreements remain between civil service and civil society actors over the most appropriate ways to safeguard privacy in the burgeoning eGovernment environment. However, there was near unanimity across groups in claiming that the restrictions stemming from such concerns were not necessarily impediments to the implementation of online services. When asked whether the architecture for eGovernment in Denmark had effectively been imposed by data protection legislation, the emphatic response was that “it was also the most appropriate” architecture from both technical and administrative perspectives.

In keeping with our finding of an under-developed DCR as it relates to rights to information and service provision, we found very little evidence of influence from these types of claims on Danish eGovernment services. Developments of online service provision are being driven not by normative claims from the citizenry, but by an efficiency-seeking public sector. Interestingly, this has not precluded a prominent role for DCR in Danish eGovernment. With the aim of increasing service usage among citizens, and thus achieving higher efficiency gains, the Danish state has conferred rights over communications with the public sector – the “eDays”. In essence, DCR is instrumental to achieving other goals, rather than the goal in and of itself.

The lesson that we draw from this is that, far from imposing barriers, thoughtful DCR regimes can very well act as enablers to eGovernment. In order to encourage the development, implementation and uptake of eGovernment services aimed at citizens, the project team has proposed to establish an eRight for citizens to use electronic media to access public services. This recommendation is clearly related to Directive 2006/123/EC on services in the Internal Market that has included some interesting provisions addressed to Member States. These aim to facilitate the exercise of the freedom of establishment for service providers and the free movement of services, some closely related to the use of ICTs. A new Directive related to rights and freedoms of citizens following the model of Directive 2006/123/EC on services in the Internal Market could be considered by all stakeholders (please see solutions for eGovernment (deliverable 3) for more details).

Appendix

(1) Burger@Overheid – eCitizen Charter

The following is an extract from Burger@Overheid (2005).

1. Choice of Channel - As a citizen I can choose for myself which way to interact with government. Government ensures multi channel service delivery, i.e. the availability of all communication channels: counter, letter, phone, e-mail, Internet.
2. Transparent Public Sector - As a citizen I know where to apply for official information and public services. Government guaranties one-stop-shop service delivery and acts as one seamless entity with no wrong doors.
3. Comprehensive Rights and Duties - As a citizen I know which services I am entitled to under which conditions. Government ensures that my rights and duties are at all times transparent.
4. Personalised Information - As a citizen I am entitled to information that is complete, up to date and consistent. Government supplies appropriate information tailored to my needs.
5. Convenient Services - As a citizen I can choose to provide personal data once and to be served in a proactive way. Government makes clear what records it keeps about me and does not use data without my consent.
6. Comprehensive Procedures - As a citizen I can easily get to know how government works and monitor progress. Government keeps me informed of procedures I am involved in by way of tracking and tracing.
7. Trust and Reliability - As a citizen I presume government to be electronically competent. Government guarantees secure identity management and reliable storage of electronic documents.
8. Considerate Administration - As a citizen I can file ideas for improvement and lodge complaints. Government compensates for mistakes and uses feedback information to improve its products and procedures.
9. Accountability and Benchmarking - As a citizen I am able to compare, check and measure government outcome. Government actively supplies benchmark information about its performance.
10. Involvement and Empowerment - As a citizen I am invited to participate in decision-making and to promote my interests. Government supports empowerment and ensures that the necessary information and instruments are available.

(2) Westen – Digital Citizens' Bill of Rights

The following is an extract from Westen (2006).

1. Right to Information

- Right to identify the name, title, contact information and duties of each elected official directly responsible to each citizen (e.g., a citizen should be able to access an online government database, enter his/her address and identify their city council member, county supervisor, state assembly member, etc.)
- Right to obtain elected officials' voting records and positions on range of issues
- Right to access full-texts of all government research online and, where feasible, through other media (TV, Video-on-Demand)
- Right of access to online search engine to locate government research

- Right of access to government information in multiple languages where appropriate (e.g., English & French in Canada)

2. Right to Transparency

- Right to view online agendas of all upcoming governmental meetings
- Right of notification (e.g., e-mail, text message), upon request, of specific upcoming governmental decisions (e.g., citizens would indicate they are interested in specific issues, and city council would e-mail them notification a week before issues are considered, so citizens can participate in public hearing or comment by e-mail)
- Right to access online streamed and/or archived video coverage of public government decisions (e.g., video coverage of city council, state legislature), via TV, the Web or Cable TV/DBS/Cellular Video-on-Demand retrieval systems

3. Right to Petition

- Right to access software that will allow citizens to transmit their opinions on pending issues to government officials
- Right to expect that information transmitted to elected officials electronically will not be ignored (officials will log comments, respond in timely manner, etc.)
- Right to participate in periodic, online, non-binding government-initiated public opinion polls, to express opinions on major items pending before local, regional, state and national governments (e.g., government would conduct public opinion polls, post the results, and publicly respond through committee hearings, legislative resolutions, etc.) (alternative to binding ballot initiative)

4. Right to Vote

- Right to vote online in manner that is private, secure and accurate
- Right to sign online petitions to qualify citizen initiatives for the ballot, in jurisdictions which utilize the ballot initiative process
- Right to receive voter information on all candidates for elected office and ballot measures in textual and/or video formats via the Web, Internet or Cable TV/DBS/Cellular Video-on-Demand retrieval systems

5. Right to Privacy

- Right to inspect any information collected by government and to correct it for errors or omissions
- Right to prevent government and private vendors from selling, disseminating or making public any private information collected by government, where that information personally identifies specific citizens

6. Right to Access

- Right of universal access to government information and services via the Internet (e.g., free government supported public points of access through libraries, kiosks, etc.)
- Right of access to government via electronic technologies (e-mail, Internet) should exist irrespective of age, gender, race, income or disability (e.g., voice activation for blind, sub-captioning for deaf)
- Right to receive free government-supplied e-mail addresses and accounts
- Right to explicit governmental policies designed to keep Internet access costs low (tariffs, antitrust enforcement policies against media monopolization, etc.)

7. Right to Assemble

- Right to create or join online communities and forums without constraint
- Right to privacy in online memberships

8. Right to Freedom of Expression

- Right to free and uncensored personal communication without governmental intervention
- Right to free and uncensored communication in un-moderated public forums or networks

9. Right to Online Services

- Right to enter into government transactions (e.g., income tax filing) or obtain government services (e.g., auto registration) online
- Right to obtain online answers to specific questions relating to government (e.g., hours of park operation, ways to obtain camping permits)

EUROCITIES – Charter of Rights of Citizens in the Knowledge Society

The following is an extract from EUROCITIES (2005):

Chapter I. Rights to Access

1. Every citizen of the European Union will have access to the Internet through Public Internet Access Points, preferably via a broadband network.
2. Every citizen of the European Union must be guaranteed the security and privacy of any personal data managed through online public services.

Chapter II. Rights to Education and Training

3. Every citizen of the European Union will have the right to acquire the basic skills for an effective use of services and information through ICT.
4. Every citizen of the European Union will have access to personalised assistance when accessing public and ICT-based equipment and facilities.
5. Every citizen of the European Union will have access to lifelong e-learning platforms to benefit from all the available resources generated by communication technology facilities and thus take part in the Knowledge Society.

Chapter III. Rights to Online Information

6. Every citizen of the European Union will have access to the best quality information produced by public administrations.
7. Every citizen of the European Union will have access to online information regardless of disabilities.

Chapter IV. Rights to Online Participation

8. Every citizen of the European Union will be ensured the right to participate through ICT platforms in the decision-making processes of his or her local government.
9. Every citizen of the European Union will receive public administration feedback on any online consultation results.

References

Bovens, Mark. 2002. “Information Rights: Citizenship in the Information Society”, Journal of Political Philosophy 10(3), pp. 317-341

Burger@Overheid. 2005. Workbook of eCitizen Charter of.... URL: http://www.burger.overheid.nl/files/burgerservicecode_uk.pdf (accessed 2007/04/07).

Council of Europe. 1950. European Convention on Human Rights. (Also known as the Convention for the Protection of Human Rights and Fundamental Freedoms.) URL: http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (accessed 2007/04/04).

Directive 2006/123/EC of 12 December 2006 on services in the Internal Market Official Journal of the European Communities L376, 27/12/2006, pp. 36–68, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_376/l_37620061227en00360068.pdf

Drake, William J. and Rikke Frank Jørgensen. 2006. “Introduction”, in Rikke Frank Jørgensen (ed.), Human Rights in the Global Information Society, London: MIT Press.

Dworkin, Ronald. 2005. Taking Rights Seriously. Universal Law Publishing Co Ltd.

EUROCITIES. 2005. Charter of Rights of Citizens in the Knowledge Society. URL: http://www.eurocities.org/uploads/load.php?file=know_charter_eRights_final-SMu.pdf (accessed 2007/04/07).

European Union. 1995. Directive 95/46/EC. URL: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm (accessed 2007/04/04).

European Union. 2000. The Charter of Fundamental Rights of the European Union. URL: http://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed 2007/04/04).

Government of Denmark. 2002. Citizens at the Wheel. URL: http://www.moderniseringsprogram.dk/visPublikation.asp?artikelID=5187 (accessed 2007/02/17)

Hoff, Jens, and Jacob Rosenkrands. 2000. 'When democratic strategies clash: The citizen card debate in Denmark' in Jens Hoff, Ivan Horrocks, and Pieter Tops (eds.), Democratic Governance and New Technology: Technologically mediated innovations in political practice in Western Europe.

Knowles, Dudley. 2001. Political Philosophy. London: Routledge.

Marshall, T.H. and Tom Bottomore. 1991. Citizenship and Social Class. Pluto Press.

McIver, William J., William F. Birdsall, and Merrilee Rasmussen. 2003. “The Internet and the right to communicate”, *First Monday* 8(12)

Ministry of Interior & Health. 2006. The local government reform – In brief. URL: http://www.im.dk/publikationer/government_reform_in_brief/Kommunal_UK_screen.pdf (accessed 2007/03/17)

Moore, Nick. 1998. “Rights and Responsibilities In An Information Society”, Journal of Information, Law and Technology 1998(1). URL: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_1/moore/ (accessed 2007/04/09).

Poelmans, Matt. 2004. “Making eGovernment work: the content and the significance of an eCitizen's Charter”, in Willi Kaczorowski (ed.), *Connected Government*, London: Premium Publishing.

Thompson, Marcelo. 2006. Property Enforcement or Retrogressive Measure? Copyright Reform in Canada and the Human Right of Access to Knowledge. uOttawa LLM Research Paper.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, Conference of the Representatives of the Governments of the Member States, Brussels 3 December 2007, http://www.consilium.europa.eu/uedocs/cmsUpload/cg00014.en07.pdf

United Nations. 1948. Universal Declaration of Human Rights. URL: http://www.un.org/Overview/rights.html (accessed 2007/04/04).

United Nations. 1966. International Covenant on Civil and Political Rights. URL: http://www.unhchr.ch/html/menu3/b/a_ccpr.htm (accessed 2007/04/04).

United Nations. 1966b. International Covenant on Economic, Social and Cultural Rights. URL: http://www.unhchr.ch/html/menu3/b/a_cescr.htm (accessed 2007/04/04).

Westen, Tracy. 2006. A Digital Citizens' Bill of Rights. URL: http://www.cgs.org/publications/articles/Digital_Citizens_Bill_of_Rights.pdf (accessed 2007/04/04).

WSIS. 2003. Declaration of Principles. URL: http://www.itu.int/wsis/docs/geneva/official/dop.html (accessed 2007/04/04).