Prepared for the eGovernment Unit
DG Information Society and Media
European Commission

Breaking Barriers to eGovernment

Overcoming obstacles to improving European public services

Modinis study

Contract no. 29172

Solutions for eGovernment

Deliverable 3

23/12/2007

eGovernment Unit
DG Information Society and Media
European Commission

Section 1: Executive Summary

The Internet and related electronic information and communication technologies (ICTs) are being used increasingly in Europe to enhance the delivery of public services and citizens' democratic engagements with government. However, many proponents believe that progress in eGovernment has been hampered by legal, organizational and other obstacles.

The Breaking Barriers to eGovernment project was funded by the EC for three years to address this issue. The overall objective of the research is to identify and explore the barriers to eGovernment progression in Europe and suggest organizational and legal solutions to overcome these obstacles. Three research reports have been produced by the project team: a legal and institutional analysis of barriers to eGovernment (deliverable 1b); a case study report (deliverable 2); and a solutions report (deliverable 3).

The focus of this report, Solutions for eGovernment, is the identification and recommendations of key legal and organisational solutions to overcoming the barriers to eGovernment, such as creating a network of eGovernment champions and establishing a citizen's 'eRight' to access public services electronically. These recommendations are based on results from the European Commission's 'Barriers to eGovernment' project. These recommendations aim to further the objectives of the European Commission's i2010 eGovernment Action Plan that were developed and reinforced by the Lisbon Ministerial Declaration of the 19th of September 2007: leaving no citizen behind; making efficiency and effectiveness a reality; implementing high-impact key services for citizens and businesses; putting key enablers in place; and strengthening participation and democratic decision-making.

The first section of this report highlights the two main dimensions to the project's results: the seven major barrier categories identified by the project; and eight key legal areas analysed in detail. Solutions arising from the research are then presented, starting with suggestions for organizational approaches to address a key barrier within each of the seven barrier categories. Summaries are then provided of some key solutions to facilitate smoother eGovernment progress through legal adaptations at European, national, regional and local levels.

Partners

The Breaking Barriers project is led by the Oxford Internet Institute (OII), University of Oxford (http://www.oii.ox.ac.uk) and has four project partners. They are:

- Centre de Recherches Informatique et Droit (CRID), University of Namur, Belgium (http://www.fundp.ac.be/facultes/droit/recherche/centres/crid/)
- Department of Administrative Law, University of Murcia, Spain (http://www.um.es/dereadmv)
- Gov 3 Ltd, London, UK (http://www.gov3.net)
- Tilburg Institute for Law, Technology, and Society (TILT), University of Tilburg, Netherlands (http://www.uvt.nl/tilt)

Acknowledgements

The project team would like to thank Dr Trond-Arne Undheim from the eGovernment Unit at the European Commission and all members of the expert group for their valuable contributions to the study through their participation via interviews, presentations at workshops and comments on a previous editions of this and other reports from the barriers project (see: http://www.egovbarriers.org/?view=Expert&type=GroupList).

Full details of the project, partners, papers, resources and events are available on the project website at: http://www.egovbarriers.org.

Section 2: Introduction

The delivery of improved public services and support for active democratic engagement can be enhanced through eGovernment: the use in public administrations of information and communication technologies (ICTs), such as the Internet, together with relevant associated organizational change and skills development (European Commission 2003). The adoption and implementation of appropriate eGovernment policies and practice in Europe would make a significant contribution to fulfilling the Lisbon Strategy of making the EU "the most competitive and dynamic knowledge-based economy with improved employment and social cohesion by 2010" (European Commission 2002).

However, there are numerous obstacles that can hinder progress towards realizing the promise of eGovernment, as has been recognized within the EU through various related Directives, communications and research initiatives (European Commission 2003; OECD 2003; Australian Government Information Management Office 2003; IPTS 2004). Substantial legal, political, administrative, social, institutional and cultural differences between Member States and regions (Leitner 2003; Graafland-Essers and Ettedgui 2003) in the EU make such understanding of the main impediments to eGovernment of particular relevance to the growing number of important public services that seek to span national and regional boundaries. New initiatives are also often needed when rapid technologically-enabled change creates problems by outpacing the evolution of legal and organizational arrangements.

In 2005 a three year study funded by the European Commission, the Breaking Barriers to eGovernment project, was launched. The overall objective of the research was to identify and explore the barriers to eGovernment progression in Europe and suggest organisational, technical and legal solutions to overcome these obstacles. The project team have used four main methods to achieve these aims: a critical review of a wide collection of existing work on eGovernment, a non-probabilistic web-based survey, case study research and engagement with eGovernment experts via a project website, six-monthly workshops, and the creation of an expert group.

This report, Solutions for eGovernment, sets out the solutions proposed by the project team. The report is divided into four parts. In this part the framework and concepts developed and utilised by the project team for this research project is summarised. The second part focuses on organisational solutions, the third part explores the legal solutions and the final part provides a conclusion to the research.

Definition of an eGovernment barrier

For the purposes of this project a barrier has been defined as:

> *Characteristics – either real or perceived – of legal, social, technological or institutional context which work against developing eGovernment, either: because they impede demand, by acting as a disincentive or obstacle for users to engage with eGovernment services; or because they impede supply, by acting as a disincentive or obstacle for public sector organizations to provide eGovernment services.*

The seven barrier categories

The project team have identified 7 key barrier categories which provide a simple guide to an almost infinite list of possible barriers to eGovernment. These were initially developed via an iterative process from analysis of previous work in this area and discussions with experts. The categories were developed and refined through the online survey and case study work carried out by the project team.

The seven barrier categories are:

- Leadership failures: Slow and patchy progress to eGovernment can result from a lack of adequate leadership during any stage in the initiation, implementation, promotion and ongoing support of developments.

- Financial inhibitors: Concerns about the costs of implementing and developing eGovernment, together with inappropriate cost/benefit analysis approaches, can constrain or block the flow of investment at the levels necessary to support future eGovernment innovation.

- Digital divides and choices: Inequalities in skills and access can limit and fragment take-up of eGovernment. Failure to address clearly the needs of potential eGovernment users can also hamper take-up of eGovernment as even those citizens and businesses with appropriate levels of access may choose not to use available eGovernment services.

- Poor coordination: Lack of coordination and harmonization can put a brake on establishing appropriate eGovernment networks and services that cross governance, administrative and geographic boundaries.

- Workplace and organizational inflexibility: The realization of eGovernment benefits can be constrained or blocked by inflexibilities in responding to the need to make necessary changes in public administration practices, processes and organizational structures to allow them to be better able to make appropriate effective use of electronic networking capabilities.

- Lack of trust: Heightened fears about inadequate security and privacy safeguards in electronic networks and a general distrust of government can undermine confidence in eGovernment.

- Poor technical design: Interoperability blockages caused by incompatibilities between ICT systems or difficult-to-use interfaces to eGovernment services exemplify the kinds of practical flaws that can become serious operational obstacles to take-up of what otherwise appear to be valuable eGovernment systems.

The eight legal foundations

The legal context and the ways in which legal frameworks can facilitate or hinder eGovernment developments is a key area of this study. Thus, the project team have identified 8 legal foundations of the 7 barrier categories that can facilitate or block eGovernment progress. They are:

- Administrative law in many European countries that recognizes certain formal guarantees which can create legal ambiguities and obstacles for some eGovernment services.

- Authentication and identification: procedures to check identities of online users, which can become barriers if they are too costly or cumbersome.

- Intellectual Property Rights (IPR): protecting creative works, which can impair flexibility and fairness in some eGovernment applications.

- Liability laws: addressing complex new divisions of responsibility in online relationships between government, businesses and citizens.

- Privacy and data protection rights: facilitating or blocking information sharing in eGovernment activities.

- Public administration transparency: such as Freedom of Information laws that can add costs as well as giving greater access to government information.

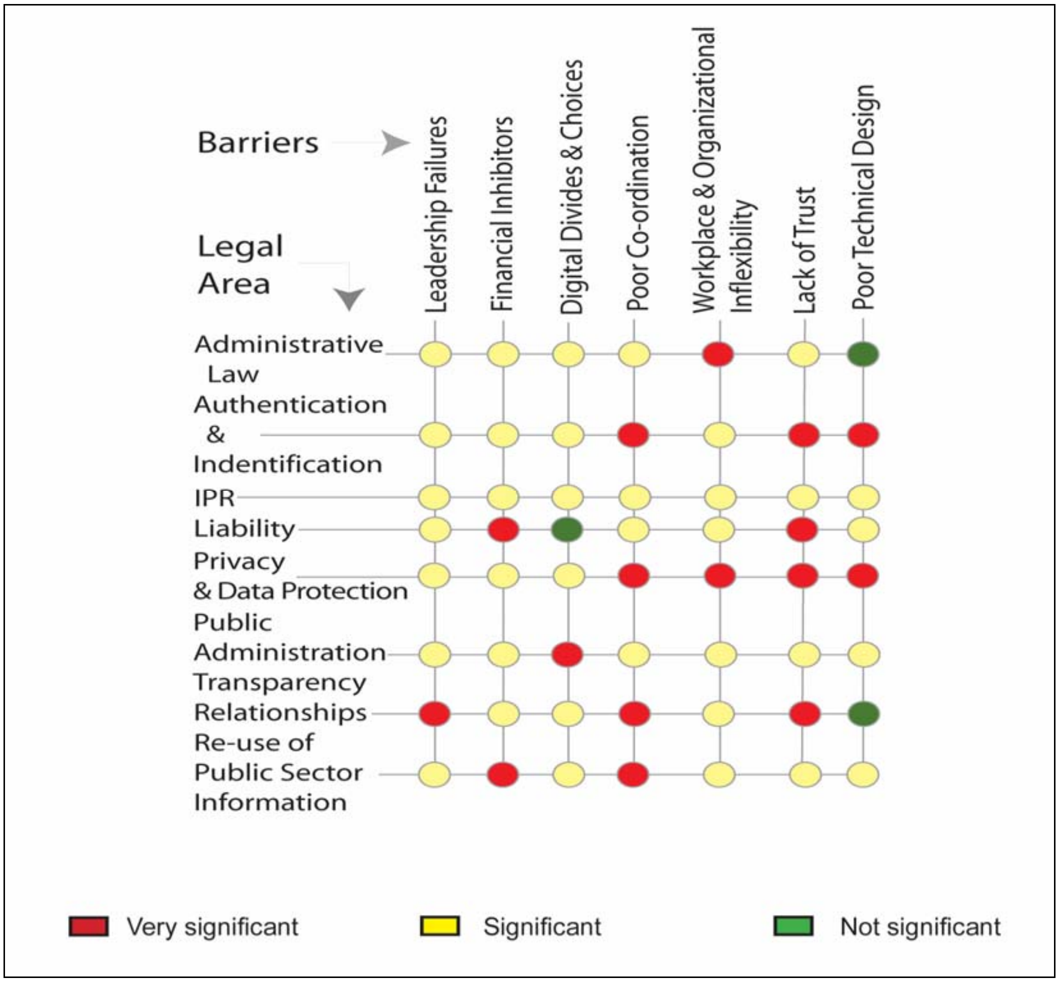
- Relationships between public administrations, citizens and other ICT actors: such as a general right to use online services or contractual arrangements between public administrations and ICT suppliers.

- Re-use of public sector information: which can raise complex legal issues when information from networked computer systems and databases can be accessed from different jurisdictional and organizational contexts.

For more details of the barrier categories and legal areas please see a legal and institutional analysis of barriers to eGovernment (deliverable 1b).

The relationship between the barrier categories and the legal foundations

Table 1 illustrates a simplified rating of the significance of the main legal dimensions to the seven barrier categories we have highlighted. This table uses a traffic light system to indicate the level of significance each legal area has for each eGovernment barrier category. From the table it can be seen, for example, that liability and re-use of public sector information are the most significant legal dimensions for financial barriers to eGovernment. More legal dimensions have crucial implications for the lack of trust barrier: authentication and identification; liability; privacy and data protection; and relationships between public administrations, citizens and other ICT actors. We believe this table is useful as it offers some valid broad indicators, but should not be taken as precise and definitive evaluations of what are complex and highly subjective assessments.



Barriers → Legal Area ↓	Leadership Failures	Financial Inhibitors	Digital Divides & Choices	Poor Co-ordination	Workplace & Organizational Inflexibility	Lack of Trust	Poor Technical Design
Administrative Law	🟨	🟨	🟨	🟨	🟥	🟨	🟩
Authentication & Indentification	🟨	🟨	🟨	🟥	🟨	🟥	🟥
IPR	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Liability	🟨	🟥	🟩	🟨	🟨	🟥	🟨
Privacy & Data Protection	🟨	🟨	🟨	🟥	🟥	🟥	🟥
Public Administration Transparency	🟨	🟨	🟥	🟨	🟨	🟨	🟨
Relationships	🟥	🟨	🟨	🟥	🟨	🟥	🟩
Re-use of Public Sector Information	🟨	🟥	🟨	🟥	🟨	🟨	🟨

🟥 Very significant 🟨 Significant 🟩 Not significant

Table 1 Relationships between barriers and legal areas

The development of solutions for eGovernment

The development of table 1 and the research behind it assisted the project team in understanding that each category of barrier to eGovernment is related to most if not all of the 8 legal foundations. Moreover, each legal area, such as IPR, is viewed to be significant to most categories of barriers to eGovernment. Thus, there are no simple 'single-bullet' solutions for defeating the obstacles to effective eGovernment across Europe. On the contrary, the barriers to eGovernment are multiple, interrelated and resistant to change.

The project team have developed one organisational solution for each barrier category and at least two legal solutions for each legal area. The team was not, therefore, aiming to produce solutions to all the potential problems of eGovernment, but to identify a range of tangible solutions to specific barriers.

The organisational and legal solutions were based on first identifying the most important barriers within each barrier category via the reviews of existing work in this field, the online survey, the case study research and discussions with experts. Then, using the findings from the research and the expertise of the project partners the solutions were developed, then discussed with experts, and revised accordingly.

In parts two and three of this document the specific solutions are put forward. In the first, organizational solutions to barriers to eGovernment are presented and in the second the project team's main proposals for actions at European, national, regional and local levels to adapt legal frameworks to facilitate smoother eGovernment progress are summarized. The recommendations indicate who (e.g. European Commission or Member States) should act on the proposals suggested. These recommendations aim to further the objectives of the European Commission's i2010 eGovernment Action Plan: leaving no citizen behind; making efficiency and effectiveness a reality; implementing high-impact key services for citizens and businesses; putting key enablers in place; and strengthening participation and democratic decision-making that were reinforced by the Lisbon Ministerial Declaration of the 19th of September 2007.

References

Australian Government Information Management Office (2003), EGovernment Benefits Study, http://www.agimo.gov.au/publications/2003/03/e-govt_benefits_study

European Commission (2002), Communication on eEurope 2005: An Information Society for All, http://europa.eu.int/information_society/eeurope/2005/all_about/action_plan/index_en.htm

European Commission (2003), The Role of eGovernment for Europe's Future, COM (2003) 567, http://europa.eu.int/information_society/eeurope/2005/doc/all_about/egov_communication_en.pdf

European Commission (2006), i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, Brussels: European Commission, http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/egov_action_plan_en.pdf

European Ministers (2007), Ministerial Declaration approved unanimously at the 4th Ministerial eGovernment Conference in Lisbon, Portugal, http://www.epractice.eu/document/3928.

Graafland-Essers, I. and Ettedgui, E. (2003), Benchmarking E-Government in Europe and the US, http://www.rand.org/publications/MR/MR1733/MR1733.pdf

IPTS (2004), eGovernment in the EU in 2010: Key Policy and Research Challenges – Workshop Report. European Commission, JRC, Seville, Spain, August, Brussels: Institute for Prospective Technological Studies (IPTS).

Leitner, C. (2003), eGovernment in Europe: The State of Affairs, http://www.e-europeawards.org/view_extern.asp?id=4706

OECD (2003), the eGovernment Imperative, Paris: OECD, http://webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf/viewHtml/index/$FILE/publications.htm

Section 3: Solutions for the seven eGovernment barriers

In this section, we propose solutions to some of the barriers to eGovernment identified in the course of the project. We outline each of the seven categories of barriers that we identified earlier in the study, and for each category, we nominate a key barrier – and identify a solution to that barrier.

The seven barrier categories are:

- Leadership failures
- Financial inhibitors
- Digital divides and choices
- Poor coordination
- Workplace and organizational inflexibility
- Lack of trust
- Poor technical design

We are not, therefore, aiming to produce solutions to all the potential problems of eGovernment, but to identify a range of tangible solutions to specific barriers. For each solution that we propose, we give some examples of where it has been used and make a recommendation to the Commission in terms of encouraging its take-up across member states.

Leadership Failures

eGovernment progression can be limited by failures in political and management leadership (e.g. OECD 2003a, United Nations 2003). Indeed, the Lisbon Ministerial Declaration of the 19th of September 2007 highlighted the importance of strong leadership to ensure transformational change that harnesses the value of new technologies. Successful leadership requires an ability not only to manage complex ICT projects but to motivate and support sustained commitment to eGovernment within public administrations and the use of eGovernment services by citizens. There is also a need to effectively manage differences in interests; perceptions and understanding among different stakeholders to ensure such conflicts do not become blockages to eGovernment.

Leadership failure can lead to low prioritization of eGovernment in public policies and resource allocation; lack of integration of the eGovernment agenda with mainstream strategies for public sector reform; poor senior management understanding of eGovernment; and poor strategic vision and planning. Basically, eGovernment needs champions. Political support from the top is an important (identified as such by 68 % of participants in the Breaking Barriers project online survey[1]) but not a sufficient condition to overcome leadership failures; it may indicate the presence of a champion at the highest levels of government, but it can be difficult to sustain or to feed down to other tiers of government without a seam of personnel throughout departments and agencies who prioritise eGovernment issues. Lack of sustained leadership for eGovernment will lead to cycles of attention and inattention that lead to patchy, stop-go progress.

[1] For the survey report please see: http://www.egovbarriers.org/?view=project_outputs. All further references to this survey will be indicated by the phrase "project survey".

Key Solution: Creating a Network of eGovernment Champions

One way of sustaining attention to and prioritisation of eGovernment is the creation of a Chief Information Officer (CIO) role throughout government organizations, as in most private companies and as (for longer than in any European country) in US federal departments and agencies. Such a role should not be restricted to one per department, but should also be created in agencies and public bodies and even, for very large departments, at division or bureau level, so that there is a 'seam' of eGovernment champions throughout public administration, ready to promote eGovernment initiatives.

Such a strategy would complement the current i2010 eGovernment subgroup who report to the High Level Group on the implementation of the i2010 eGovernment Action Plan. The sub-group is made up of eGovernment leaders and national representatives from Member States and Accession Countries which are members of the i2010 High Level Group. The creation of a seam of CIOs throughout government in all member states would complement and assist the i2010 eGovernment group, providing input when needed and ensure the work of the i2010 eGovernment subgroup has an influence at all levels and departments within government (European Commission 2006b).

There are two elements that must be built into the creation of a CIO network. First, some cross-departmental forum of CIOs must be built into the routine of a government administration on a regular basis, so that CIOs are continually aware of developments in other departments and possible synergies between initiatives and projects are highlighted. In the UK, such fora have facilitated discussion, awareness and even cross-departmental working on eGovernment issues between (for example) taxation and benefit agencies, to a greater extent than ever before. Second, it must not be assumed that the departmental CIO is the only official from a department who should attend the highest level CIO meetings. In some cases, the IT budget of an agency will be far larger and more policy-critical than the budget of the parent department (the taxation agency is likely to have a larger IT budget and role than a Treasury department, for example) and no government wide discussion of eGovernment issues should take place without the presence of this agency's CIO.

CIOs were introduced in many US federal government agencies from the early 1990s and the Clinger-Cohen Information Technology Management Reform Act of 1996 mandated provision for CIOs as information change agents and 'technology watchdogs' across the federal government (Buehler 2000). Their creation was aimed at ensuring that 'a CIO has a powerbase as a major participant in agency management', arising from concern over the earlier practice of Information Resource Management (IRM) officials acting as top information persons in the majority of agencies and departments, who were essentially "techies" who held the philosophy of 'IT for IT's sake' (Buehler 2000).

Strong and competent leadership by CIOs has a positive influence on the success of eGovernment (Seifert and McLoughlin 2007). However the effectiveness of the implementation of CIOs as a consequence of the Clinger-Cohen Act has varied from agency to agency. One key issue to explain this diversity is the specific role the CIO has within the agency (e.g. Kost 2005; Liu and Hwang 2003) Indeed, a lack of clarity regarding the CIOs role, the relationship of the CIO to other existing IT management initiatives at that time, the placement of the CIO in the agency hierarchy and uneven budget allocations have all been identified as potential brakes on the establishment and impact of CIOs in federal government when the act was first implemented (McClure and Berot 2000). The issue noted above of disparity between IT budgets across the hierarchy has been important; the Federal Aviation Administration, for example, has a far greater e-government role than the Department of Transportation and their absence at departmental CIO meetings has caused problems in the past. A related issue is the importance of the CIO having support from the agency head and the senior management team (Moore 2004). Thus, the effectiveness of the CIO position is not just about the competences of the individual, but their place with the government agency and the resources they have at their disposal.

Mechanisms should also be put in place for communication between those championing specific eGovernment initiatives, therefore increasing the likelihood of 'joined-up' or 'seamless' government. In the UK from 2004, the CIO Council was set up to ensure that CIOs 'operate on a "collective responsibility" basis to steer, own and deliver agreed strategic actions' (www.cio.gov.uk). It meets for a minimum of three full days a year, with CIOs attending in purpose, thereby ensuing that the CIOs of major departments meet on a regular basis and facilitating the discussion of common issues. It plays a role in consolidating the public sector IT profession, particularly through contributing to the Professional Skills for Government agenda, thereby reinforcing the concept of a network of IT professionals across UK government. But most importantly, it facilitates communication and discussion between IT divisions of departments that formerly were unlikely to do so, giving rise to cross-departmental eGovernment initiatives and strategies.

One way of drawing attention to and incentivizing champions at any level of administration is to introduce prizes for eGovernment development. In Denmark, for example, the "Best on the Internet" initiative gives ratings of public homepages and thereby encourages authorities to prioritize usability of their websites; and secondly the "Prize of eGovernment" is given to public institutions in three categories "Efficient eGovernment and service to citizens", "Coherence of IT Infrastructure" and "Good eGovernment Leadership". In Germany, the BundOnline Star is awarded twice a year to recognise excellence of a service and its implementation in three categories (G2C, G2B, G2G) by the Ministry of the Interior following a vote by the Institute of Electronic Business in Berlin. The Federal Ministry of the Interior awards annually a set of prizes within its eGovernment competition. Participants come from all levels of the administration (federal, regional and local) and prizes are assigned in four categories (G2C, G2B, G2G and G2E). The competition is organized together with partners (Cisco, BearingPoint) and prizes are awarded during the CeBIT fair. Italy also has a number of awards, for example I Successi di Cantieri, organized by the Department of public administration, (http://www.cantieripa.it/inside.asp?id=204); COMPA assigns awards to administrations in the innovation area of citizen-administration relationships including on-line communication (www.compa.it); and EuroPA assign awards to best websites of local administrations (www.euro-pa.it).

Recommendation: Creating champions for eGovernment across public administration is one way to ensure that the objective of 'making efficiency and effectiveness a reality' is achieved, through the prioritisation of eGovernment issues at the highest levels of public organisations' strategies. In future guidance to member states on the development of eGovernment, the European Commission recommend the creation of CIOs, at least at departmental level.

Financial inhibitors

The costs of developing, implementing and maintaining eGovernment (e.g. costs of software, hardware and training for government officials) can be important financial inhibitors. Furthermore, difficulties in calculating tangible long term benefits to offset clear, often apparently high, short term costs can severely hamper the speed and scope of eGovernment progress; particularly when spending on eGovernment competes with other critical demands on public resources (e.g. building roads or schools). Understanding both costs and benefits can help to inform eGovernment expenditure, yet such analysis is complex and rarely undertaken. Difficulty in demonstrating the cost benefits of eGovernment initiatives was considered an important or very important barrier by 60% of project survey participants.

Key Solution: Calculating the Benefits

Working out the benefits of eGovernment (including the risks of not developing and innovating) is as important as working out the costs. As noted by the Lisbon Ministerial Declaration of the 19th of September 2007 the measurement of the impact of eGovernment is a key area. As eGovernment developments progress, working out the benefits becomes increasingly important, as it becomes more difficult to cost-justify investment in eGovernment through 'conventional' savings such as reduction in staff costs for administrative operations, through which IT projects have traditionally been cost-justified. Private corporations calculate the 'asset value' of web sites and electronic services – governments should do the same, taking account of the real public value of easily available, visible, accessible and navigable government information.

Possible strategies for estimating asset values (Dunleavy 2006) include:

- Taking asset values as a multiple of income generated from the resource – e.g. company websites are often valued at between 2 and 6 times the income generated. In the public sector some agencies have near-commercial activities where a direct read-across of corporate asset valuation methods might be appropriate. But most government agencies pay out or expend money rather than collecting it. At the other extreme, taxing agencies pull in high yields via eProcesses – but they commonly apply tests that restrict their administrative costs to a fraction of revenues generated – e.g. the rule that the marginal tax officer must generate 8 times their salary in revenues. The same rule might be applied to eResources and IT investments for taxing agencies.

- Imputing a positive value per thousand visitors to websites on grounds going beyond simple income – e.g. taking account of brand recognition, market positioning, goodwill, protection against competitors, or the ability to leverage other corporate benefits from contact with customers or potential customers.

- Assessing what it would cost to run the organization's operations without the web site. The more digitally-based an agency becomes, the larger this asset value would be. This has the advantage of signalling greater risks the more dependent an agency is on eProcesses and hence a greater need to make IT investments as digitalization proceeds and conventional processes dwindle. However, the high transaction costs (and utopianism) of re-establishing conventional processes once some operation has been digitalized may tend to inflate asset value estimates unrealistically. Possibly once could strip out transactions costs, but the resulting numbers would then be rather theoretical or notional only. Do private sector companies use this approach at all and how do they then fit it to their specific position and industry so as to achieve realistic results?

Recommendations: Furthering the objective of implementing high-impact key services for citizens and businesses will only be achieved if the positive impact of key services can be measured. Methodologies for calculating public sector asset value is an underdeveloped area of public administration research. The EC should commission research on methods of calculating the asset value of public sector web sites, to complement the programme of research into common impact/benefit-oriented eGovernment measurement framework outlined in the i2010 Action Plan (European Commission, i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All 2006: 6).

Digital Divides and Choices

Social and economic divides demarcated by wealth, age, gender, disability, language, culture, geographical location, size of business and other factors – can mean eGovernment resources are used in very different ways (or not used at all) by different individuals, groups and organizations. Indeed, addressing the challenges of digital divides is highlighted as a key objective of the 2006 eGovernment Action plan in the goal: 'no citizen left behind' (European Commission 2006) and was reinforced by the Lisbon Ministerial Declaration of the 19th of September 2007. Without a more nuanced understanding of user needs and choices, uptake of eGovernment will remain limited and the potential benefits (e.g. cost reductions or greater user satisfaction) will not be realized. Two particularly important barriers of this kind are that citizens can lack strong motives to use eGovernment services (considered an important or very important barrier by 61% of project survey participants) and low levels of Internet use amongst certain groups (considered an important or very important barrier by 69% of project survey participants)

Governments need to accept that there is no simple divide between Internet access/no Internet access, but rather a segmented citizenry with quite different eGovernment needs.

Key Solution 1: Segmentation

A key way to overcome divides in digital access and choice and to increase take-up of eGovernment is to segment users of eGovernment services into specific groups and treat them in distinctive ways. Survey research suggests that in the UK, the majority of Internet users now go to the Internet first if they want to find out something they don't know already, like the name of their MP (64%) or information on their taxes (55%) (OXIS 2007). For these most ardent Internet users (which we might estimate at around a third of the population), everything should be available on-line – that is where they will expect to deal with government. They are likely to be skilled Internet users and are likely to use search engines rather than portal sites, so eGovernment information and services need to be easily visible, appearing near the top of search engine results. Other Internet users need to be persuaded that eGovernment can provide the same benefits as eCommerce or eBanking, so a targeted advertising campaign for eGovernment services could have pay-offs for this group. A significant proportion of non-Internet users know someone or some organisation who can use the Internet for them if they need it; 88% of ex-users and 73% of non users in the 2007 UK Oxford Internet Survey replied positively to this question. For this group, government needs to identify the relevant intermediaries for particular sub-groups and target them in eGovernment initiatives. They should also consider formalising on-line channels of communication for intermediaries such as Citizen Advice Bureau and Non-governmental Organisations dealing with specific groups such as the elderly.

Examples of successful segmentation include:

- Lewisham has a number of successful initiatives which have been developed alongside analysis of customer views (e.g. phone and exit surveys, annual surveys, focus group meetings and visits to community groups) See http://www.idea.gov.uk/idk/aio/87366.

- In 2004 the Office of the Deputy Prime Minister in the UK launched the eCitizen Project that aimed to explore the motives and incentives to use eGovernment services by different target groups in order to increase eGovernment take up. As a result of this research a series of best practice examples are available online for use by local authorities as to how to target and market their eServices (see http://www.e-citizen.gov.uk).

- Transport for London redesigned their website on the basis of usage statistics to meet different Internet users needs. See http://www.tfl.gov.uk/.

Recommendation: Effective segmentation is going to be a key way of ensuring that 'No citizen is left behind'. The European Commission should build segmentation into their European Initiative on eInclusion, scheduled for 2008. To kickstart this process, the OII have submitted a position paper to the consultation in August 2007 at: http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=eInclusion

Key Solution 2: Providing citizens with a right to use eServices

As noted above there are a significant and increasing proportion of the population who would turn to the Internet first for their interactions with Government; and there is another group of Internet users who could be persuaded to use eGovernment services.

In order to improve the availability and quality of online services a legal solution could be to establish an eRight for citizens to use electronic media to access public services (based on Directive 2006/123/EC on services in the Internal Market). By forcing governments to permit citizens to use eGovernment, uptake and user satisfaction are likely to be increased. Further, while such a policy is aimed at Internet users all citizens will benefit due to the efficiency gains from using ICTs to transform eGovernment.

Recommendation: We recommend the approval of a new Directive on administrative services, linked to the free movement of persons and right of establishment (using Articles from Directive 2006/123/EC as a model, where relevant). Please see the part on Relationships between public administrations, citizens and other actors in section 4 for more details.

Poor Coordination

Emerging forms of eGovernment service delivery and ways of working often cross traditional government jurisdictions and administrative and departmental boundaries, as well as having the potential to overcome geographic distance. Variations in legal, regulatory and administrative regimes on different sides of those boundaries can inhibit and block the flow of information and services through new networked governance channels at EU, Member State, regional and local levels (OECD 2003b). A lack of coordination across central, regional and local levels of government was considered an important or very important barrier by 84% of project survey participants), while co-ordination between member states and the European Commission was considered an important or very important barrier by 61% of project survey participants.

Government agencies should find ways of using the benefits of developments in the Internet and WWW to overcome coordination problems.

Key Solution: Working with Chaotic Coordination

As the Internet and associated technologies and applications have developed, there are new ways to mitigate against coordination problems across fragmented organisational arrangements. The simplest example is a web site which directs the user to a range of other sources via hyperlinks, thereby bringing together diverse information resources from different organisations in one virtual location. More recently, 'Mashup' applications have made it easier for users to be presented with a far more coherent package of information deriving from disparate sources. They can even allow field workers from different organisations on the ground to update centrally held information resources, such as the UN Refugee Agency's Google map of the disaster-torn Darfur region, which can be updated by aid agency workers and other actors in the region[2]. Such applications can be used for officials working within organisations at different levels of government, simplifying their administrative environment and creating a kind of virtual service chain for information delivery. Within web sites, effective internal search engines can make a huge difference to how officials find their way around inter-organisational networks. Portals which really link up and search across tiers of government can make uncoordinated government look coherent both from inside and outside governmental organisations.

However, this type of web-enabled 'chaotic coordination' is not an automatic by-product of developing a web presence. Organisations must think about how officials use their web sites (or protected subsections of them) as information sources, just as they do for citizens using eGovernment. Their needs must be built into the design of 'portal' or intranet sites and considered when assessing the navigability of sites. Good navigability can be aided by the optimisation of key metrics (such as maximising the size of the 'strongly connected component' and minimising the path length between any two nodes on a site, see Escher et al. 2006 for a full discussion). But for larger sites (for which it is inherently more difficult to preserve navigability) extensive usability testing will be necessary for users from a range of organisational contexts. Second, if external search engines are used then the extent to which users can find the information they need will depend on the extent to which the relevant information is held on a web site that appears high up in search engine results. So optimisation for search engines, via the creation of links and data-tags for example, is an essential part of web site development. Third, organisations of all kinds have experienced major difficulties with internal search engines, which often return irrelevant or spurious results, even where (for example) the application is 'powered by Google'. Research suggests that search algorithms that work well for the Internet as a whole do not work well when used within sites, as pages cannot be ranked so effectively (Dmitriev et al. 2006). Internal search engines must be custom built for the organisation whose web site is being searched, and can require a good deal of extremely skilled resources, so good internal search engines are expensive.

These are some examples of successful initiatives where the focus was on the web-front end with limited changes to organisational structures or where effective search and subsequent 'joining-up' of information provision has been prioritised.

- Austrian customs declaration for out-of-EU trade where there was digitisation of existing workflows and architectures and the addition of a web-based front-end;

[2] See http://www.ushmm.org/googleearth/projects/darfur/

- Public libraries in Denmark where new flexible and highly compatible eSystems have been laid on top of existing software which varies from library to library;
- The US federal government portal, usa.gov (formerly firstgov.gov) has developed a reputation as a world leader in internal search. It search engine, custom built by MSN and Vizimo, searches the entire federal, state and local governments of the US[3] in contrast to many other government sites (such as the UK www.direct.gov) which searches only its own content).

Recommendation: Most of the solutions involving chaotic co-ordination are a question of 'best practice' web development which should be a normal part of an organisation's strategy. It is difficult therefore, for the Commission to offer guidance in this area. However, the specific issue of internal search engines (or 'enterprise search' as they are known in the industry) emerges as a particular problem for governments. The European Commission could consider commissioning some best practice research into this particular issue, possibly drawing on the experience of the usa.gov site in the US. Effective search engines are vital enablers for eGovernment development.

Workplace and organizational inflexibility

Resistance to innovation by public administration management and staff can slow down, impair or prevent the necessary redesign of organizations and their processes required to deliver effective eGovernment. Such inflexibility can set up barriers to the creation and delivery of efficient and effective eGovernment services that could meet changing citizen and business needs (Margetts and Dunleavy 2002; Remmen 2006). Indeed, the dominant media-substitution paradigm in eGovernment is a likely reason for the relatively limited diffusion and impact of eGovernment compared to the equivalent network-enabled transformations in eCommerce. Instead of concentrating on the 'substitution' of electronic for paper-based services, governments need to focus on facilitating the transformation of organizations in ways enabled by ICTs like the Internet. This often entails moving away from traditional 'stove-pipe' hierarchical organizational structures towards more networked organizational forms. It is during this transition that the major barriers to organizational change become major barriers to eGovernment (Eynon and Dutton 2007).

Prevailing practices can be difficult to change as they are designed to support certain patterns of communication and information exchange, while discouraging others. eGovernment initiatives often blur these boundaries and require appropriate changes to take account of the new methods of operating and managing public services. Key barriers relating to workplace and organizational inflexibility identified in our survey were the lack of ICT skills among government officials (considered an important or very important barrier by 61% of project survey participants) and resistance to change by government officials (considered an important or very important barrier by 80% of project survey participants).

Government organizations need to be agile in the way they deal with new technologies and face the resistance of those staff who have considerable organizational learning invested in off-line channels.

Key Solution: Encouraging an 'eLiterate' Workforce

The Internet and related technologies and their widespread societal use have brought a major change to government; an injection of technology into areas of bureaucracy traditionally viewed as 'technology free'. This change has taken place at all levels of government, as even policy-makers accustomed to view information technology as a policy-neutral administrative tool are realising that policy innovation often rests on some kind of technological innovation. eGovernment development therefore will be greatly aided by a workforce trained and practised in building electronic solutions into everyday working life. This can involve training in Internet and web-related issues, as well as more innovative solutions to ensure that staff are encouraged to incorporate technological innovation into all aspects of their work. Even

[3] Please see http://en.wikipedia.org/wiki/USA.gov

encouraging staff to ‘play’ with the Internet can have an important effect on cultural resistance to eGovernment, but can also be a difficult concept for organizational cultures rooted in hierarchy and solemnity (see Margetts and Dunleavy 2002, for a full discussion of cultural barriers to eGovernment). As noted above, the creation of networks of CIOs across governmental organizations can play a role in encouraging training and professionalism in IT, but changing the organisational culture will involve lower level initiatives that penetrate areas traditionally viewed as non-technical. Some examples of attempts to bring about cultural change are as follows:

- In 2003 the French government launched an eChallenge where all government employees were invited to assess their degree of understanding of ICTs. The eChallenge website (Démarche d'Evaluation du Fonctionnaire Internaute, DEFI) contained an eAssessment which tested practical skills including Internet navigation, e-mail, online discussions and web publishing and their understanding of issues such as information systems security or data protection .

- In 2006 the Hungarian government organised eGovernment training courses for 4 500 civil servants from 700 offices. The online course taken over 3 months was organised by the Ministry of Informatics and Communications and covered various eGovernment topics, such as eAdministration, electronic signatures, certification, client portals, tools for improving the e-efficiency of local government, communication, monitoring, negotiation techniques and broadband. The design of the course was informed by prior needs analysis and learner preferences. The success rate among students who completed the course was more than 90%.

- The ‘Plan Concilia’ was an attempt to reconcile personal, work and family life in Spanish central administration. It was also adopted as a pilot-project including tele-working with a selected group of senior civil servants[4.]

Recommendation: An eLiterate workforce is going to vital in the future to maximise the benefits of eGovernment and make efficiency and effectiveness a reality. It can only really happen at organizational level, but if guidance is being issued by the Commission, the need for staff to have Internet access and be encouraged to use up-to-date applications in an unrestricted way should be built into any organizational best practice.

Lack of Trust

A lack of trust is a crucial element in the take-up and effectiveness of eGovernment services. At the heart of these concerns is a ‘trust tension’ (Guerra et al. 2003) between the need to collect data on individuals as the basis for providing services, such as health records and voter registration, and fears of data surveillance or the inappropriate secondary use of personal information in computer databases. Although increasing experience with the Internet and eCommerce in the private sector is establishing more general trust in the use of ICT-enabled networks (Dutton and Shepherd 2003); eGovernment raises particular trust concerns as so many public services require the handling of highly sensitive personal information in digital forms. Take up can be also be affected by general trends in perceptions of trust in government, such as those caused by the attitude of a public administration to transparency and openness issues. Lack of trust can be exacerbated by a ‘Big Brother’ fear of unwarranted government intrusion into private lives and business operations through the growing use of networked or integrated digital databases and intrinsic ‘cybertrust tensions’ (Dutton et al. 2005), as shown in the general desire for both privacy and security even though a degree of disclosure or loss of privacy is typically necessary (e.g. to identify the user of an online tax or welfare service).

Where possible, users of eGovernment need to be provided with ‘low trust’ options, where authentication requirements are minimised.

[4] See the evaluation report (in Spanish) at: http://www.map.es/iniciativas/mejora_de_la_administracion_general_del_estado/funcion_publica/concilia/medidas/libro_electronico/document_es/libro_electronico.pdf

Key Solution 1: Matching eGovernment to Trust Requirements (low trust where possible)

The most successful eGovernment initiatives tend to be where low levels of trust are required of both users and the providing agency; that is, authentication and identification requirements are low. Of course, for some governmental transactions (obtaining a passport or driving license, for example) 'full strength' authentication and identification procedures are necessary and citizens are required to have high levels of trust in the arrangements (in terms of security) and the agencies carrying them out (in terms of the types of information they will require). But for some transactions – paying a parking fine or a road fee, for example – only one-off transactions with low levels of authentication may be required. If citizens are assured that on-line transactions take place on a 'one off' basis, without any sharing of information with other agencies, then they may be perfectly willing to carry them out on-line.

Transactions need to be assessed for authentication requirements in a realistic way. It is unlikely, for example, that someone is going to fraudulently pay a parking fine or income tax on your behalf (indeed, when high levels of authentication using DigiD were introduced by the Dutch Tax and Customs Administration and not all citizens received their personal DigiD in time for the taxfiling deadline, the Tax Administration actually suggested that citizens use the DigiD of their neighbour!).

The history of eGovernment, however, is littered with examples of where government agencies have used inappropriate levels of authentication. In the UK, for example, during the early 2000s, HM Customs and Excise required all businesses wishing to file their sales tax (VAT) returns on-line to purchase a digital certificate to do so, a decision whose legacy probably still impacts upon very low levels of electronic filing of sales tax in the UK. Meanwhile, the then Inland Revenue agency adopted a username/password system that was much easier and cheaper to use, resulting in higher rates of electronic filing for the payment of personal income tax than that recorded for sales tax. Agencies need to think about where they need to use high levels of authentication and to share information across agencies – and where one-off low authentication transactions are possible. It can be a trade-off – with higher usage levels off-setting the inferior information collection fulfilments of such applications.

Moreover, technological developments mean that the "trust level decision" does not need to be a static, one-size-fits all approach: a number of technologies now allow very low levels of initial authentication, but use smart systems to adjust in real-time to high risk situations or patterns of customer behaviour. Pioneered in the financial services sector, these technologies have the potential to maintain high levels of security while not presenting high "trust hurdles" for the great majority of citizens to overcome.

Examples of successful low trust applications:

- Many municipalities across Europe successfully collect payments for parking tickets online with a simple one off credit/debit card payment, on a system which does not link up with any other eGovernment applications.

- Payment of the congestion charge for all vehicles entering central London from 2003 onwards is another example of a successful low-trust eGovernment application

- The government of New Zealand have issued an Evidence of Identity Standard to provide guidance for government agencies about the required process for initial establishment of an individual's identity, which starts with the premise that 'Many online services delivered by government agencies are anonymous and require no evidence of identity. Other online services have low levels of identity requirements and a username and password for ongoing confirmation of identity. PKI-based authentication is desirable only for a smaller class of services' (see www.dia.gov.nz).

Recommendation: Matching trust requirements to applications could be a key way of 'Making efficiency and effectiveness a reality', contributing to high user satisfaction and transparency and a lighter administrative burden. Identifying applications where trust requirements can be minimised – and have been in other countries or contexts - should be a built into the 'sharing of experience' (EC 2006: 6), a key element of the Commission's Action Plan (together with member states) for 2008 (EC 2006: 7). In addition, the Commission should consider commissioning research into the applicability of the risk-based smart authentications systems which are being used by some financial services companies to eGovernment.

Key Solution 2: giving the citizen "ownership" of their own data (where low trust is not viable)

Despite the points made above about the need to match eGovernment to trust requirements on a risk-based approach, there will be some transactions where strong levels of authentication are required, and where the citizen needs to entrust significant levels of sensitive personal data to the government. One emerging best practice for building trust in such situations is to establish a "shared space" between the citizen and government for such data to be managed, in which the citizen's trust concerns are addressed directly by giving them high levels of transparency and control over their data: for example, enabling them to see what data is held on them by the government, to track which parts of government are accessing their data and for which purposes, and to update key aspects of their data (e.g. change of address or circumstances). A number of governments are implementing elements at least of such an approach, and the Estonian case study undertaken as part of this project (see project deliverable 2 case study report) highlights the success of this "citizen-centric" approach to trust management there.

Recommendation: the Commission should consider commissioning research into "citizen-centric trust management" approaches, including an evaluation of the extent to which giving citizens visibility and control over key data held on them by government increases their likelihood to use eGovernment services.

Poor Technical Design

eGovernment systems and services frequently fail or perform poorly because of the inadequate design and poor technical interoperability. Difficulties caused by inappropriate user interfaces to eGovernment systems can seriously hamper relations between public agencies and citizens and businesses. Such operational problems can sabotage even potentially successful services and discourage those experiencing them from trying other eGovernment opportunities. Incompatibilities in hardware, software or networking infrastructures within and between public agencies can also cause significant problems, particularly in terms of providing pan-European services. A key barrier we identified relating to poor technical design is lack of innovation in comparison with other sectors: eGovernment technologies tend to lag behind societal use of the Internet and related technologies

Government needs to put the same resources into the design of web sites as private corporations. Government's on-line presence is the new 'window' on government, the only bit that a significant subsection of the population see – so is as important as buildings.

Key Solution: Using 'user-generated' content in eGovernment applications

New technologies and applications provide the possibility to overcome traditional design problems with eGovernment. Indeed, societal use of such technologies places pressure on government organisations to 'innovate or die' in terms of take-up of online services, because citizens are only likely to want to interact with government online using the kind of technologies they are accustomed to use in other aspects of their lives. In particular so-called 'Web 2.0' applications, involving user-generated content, 'rich' (rather than text-based) information and loosely connected information sharing communities have offered major potential for innovation in private sector organisations, bringing customers into the 'front office' of product design, and offer similar potential to government. Government organisations tend to be cautious about using such applications, which can involve the use of part-authenticated information, the 'mashing up' of public and private sector applications and the creation of 'para-organisational' forms. All these characteristics blur boundaries between public and private organisations, which may invoke resistance within public organisational culture. But if such resistance can be overcome, Web 2.0 technologies could facilitate dramatic change in government-citizen online interactions, just as, for example, social networking technologies have offered new possibilities for the creation and sustaining of social relations more generally.

Government use of Web 2.0 applications is extremely sparse at the time of writing, so for this solution we have to cast a wide net to find examples, across the private and voluntary sectors.

- Use of User Testimonials: There have been hitherto virtually no government equivalents of the popular private sector travel sites which provide opportunity for users to detail their own experience of travel and holiday products. But in the UK, a successful social enterprise site (www.patientopinion.org) provides users with the opportunity to rate hospitals, treatments and even doctors they have experienced and the UK Department of Health are now planning to incorporate a version of the site into the new 'Choices' web site. In the private sector, the controversial www.ratemyteachers.com which allows pupils and parents to rate schools and teachers has over ten million users in the US and local versions have now been established in Ireland (with nearly eight and a half million ratings), the UK, Australia, New Zealand and Canada. Government sites that provide similar opportunities for citizens to rate government services could be an important part of eGovernment in the future, particularly in countries like the UK planning to build choice into the public services, where they will be vital sources of information.

- Example of mashups: League table data on the Department for Education and Skills website uses Google Maps. Users can enter their postcode and can access a Google Map showing the location, and all the primary schools in the immediate vicinity, as pointers on the map. Users can then click through to view details about the school. The same information can be accessed in other forms (e.g. comparison tables by region). See http://www.dfes.gov.uk/performancetables/. The US Holocaust museum also offers a mashup of Google Earth and on-the-ground information from the crisis-stricken Dafur region, including photographs, eyewitness accounts and a range of data from local sources and NGOs (see www.ushmm.org/googleearth).

- Examples of RSS feeds and podcasts: RSS feeds are available to access information from: the Australian Tax Office, the Australian Government Media Release Service and the Parliament of Australia (see http://www.australia.gov.au/rss). In the US users can access RSS feeds and podcasts from the whitehouse (see http://www.whitehouse.gov/rss/) and numerous RSS feeds from usa.gov (http://www.usa.gov/rss/index.shtml).

- Examples of blogs: In 2006 the Federal Trade Commission created a blog to chronicle a series of FTC hearings about "Protecting Consumers in the Next Tech-ade" (see http://ftcchat.us/blog/).

- Examples of use of second life: the National Oceanic and Atmospheric Administration have an island in second life where visitors can, for example, view the under water world from a submarine for visitors to learn about cutting edge research in this field.

- Examples of wikis: the Defense Intelligence Agency (DIA) in the US utilises a number of web 2.0 applications such as wikis, blogs, RSS feeds and "mashups". Such tools assist with pulling together all data from human intelligence in addition to data from the Internet into one source enhancing analysis of data, improving collaboration and facilitating timely information sending and dissemination[5]. A second example is Intellipedia (a copy of wikipedia) is used by the 16 US intelligence agencies to share and assess all available information more effectively than was possible previously. It is a classified hierarchy of wiki sites on intranets. (see http://en.wikipedia.org/wiki/Intellipedia)

[5] See Feb 2007 article in computerworld http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011671.

Recommendation: Innovation should be rewarded in any attempt to benchmark eGovernment services, rather than relying on the availability of services or the sometimes non-demanding measures of sophistication used in earlier studies. Indeed, in the seventh measurement of online availability of public services a composite indicator for user-centricity was piloted and the need to define and deliver the Gov 2.0 user experience was recognised (Cap Gemini 2007). The Commission should consider building developing this kind of assessment of the extent to which services are innovative or reflect current trends in societal Internet use into benchmarking studies.

Conclusion

This short paper has identified possible solutions to the key barriers to progress in eGovernment. As noted upfront, we have not tried to solve all potential barriers to eGovernment progress, but rather have put forward what we hope are feasible, specific proposals that have been tried in one or more contexts. It is worth noting that some of the solutions put forward could be used to tackle more than one barrier. For example, some of the 'web 2.0' solutions proposed to tackle lack of innovation in eGovernment might also be used to overcome the coordination problems identified earlier. Wikis, for example, can be an excellent way to communicate information across individuals in multi-organizational contexts (across tiers of government, for example), while a mashup can be a good way to draw in and disseminate information from a range of sources (such as from some combination of public, private and voluntary sectors). Likewise, giving sustained attention to eGovernment issues by creating a network of Chief Information Officers is also likely to engender cultural change, a good way to tackle workplace inflexibility. In this way, implementation of the proposed solutions can reinforce each other and have a generalised effect in promoting IT-enabled business change across a range of government activities.

References

Cap Gemini (2007), The User Challenge Benchmarking the Supply of Online Public Services. Report of the Seventh Measurement, Available at http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf

Dutton, W. H. and Shepherd, A. (2003), Trust in the Internet: The Social Dynamics of an Experience Technology, OII Research Report No. 3, Oxford: Oxford Internet Institute, http://www.oii.ox.ac.uk/research/publications.cfm

Dutton, W. H., Guerra, G. A., Zizzo, D. J. and Peltu, M. (2005), 'The Cybertrust Tension in eGovernment: Balancing Identity, Privacy, Security', Information Polity 10: 13-23.

Dutton, W.H. and Helsper, E. (2007), Oxford Internet Survey 2007 Report: The Internet in Britain (Oxford Internet Institute).

eGEP (2006), eGovernment Economics Project (eGEP) Economic Model: Final Version, 31 May, http://217.59.60.50/eGEP/Static/Contents/final/D.3.3_Economic_Model_Final_Version.pdf

Escher, T., Margetts, H., Cox, I. and Petricek, V. (2006), Governing from the Centre? Comparing the Nodality of Digital Governments. Paper resented at the Annual Meeting of the American Political Science Association (APSA) in Philadelphia (31. August - 4. September 2006).

European Commission (2006a), i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/egov_action_plan_en.pdf

European Commission (2006b), i2010 High Level Group: eGovernment subgroup Mandate, http://ec.europa.eu/information_society/eeurope/i2010/docs/high_level_group/e_government_sub-group_mandate.pdf

Eynon, R and Dutton, W. (2007), 'Barriers to Networked Governments: Evidence from Europe.' Prometheus, 25(3) 225-243

Guerra, G. A., Zizzo, D. J., Dutton, W. H. and Peltu, M. (2003), Economics of Trust: Trust and the Information Economy, DSTI/ICCP/IE/REG (2002)2, OECD, Paris.

Kost J. (2005) Government CIO Position Continues to Mature. Gartner Report. Available at, http://www.gartner.com/resources/132100/132160/government_cio_position_cont_132160.pdf

Liu, S. and Hwang, J.D. (2003), Challenges to transforming IT win the US government IT professional vol:5 iss:3 pg:10 -15

Margetts, H. and Dunleavy, P. (2002), Cultural Barriers to eGovernment, Academic Article, accompanying the National Audit Office report Better Public Services through eGovernment, London: TSO.

McClure C R and Bertot J C (2000), The chief information officer (CIO): assessing its impact Government Information Quarterly Volume 17, Issue 1, Pages 7-12

Moore, A. (2004), Role of the CIO in Electronic Government – USA. Presentation at the Worldbank seminar, "Strengthening e-Government Leadership: Emerging Role of the Chief Information Officer in the Public Sector, September 22nd 2004 Washington USA

OECD (2003a), Challenges for eGovernment Development, 5th Global Forum on Reinventing Government, Mexico City, 5 November, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan012241.pdf

OECD (2003b), The eGovernment Imperative, Paris: OECD, http://webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf/viewHtml/index/$FILE/publications.htm

Remmen A. (2006), Images of eGovernment: Experiences from Digital North Denmark, in Hoff, J. (ed) (2006), Internet, Governance and Democracy, Nias: Denmark

Seifert, J. W. and McLoughlin, G. J. (2007), State eGovernment Strategies: Identifying Best Practices and Applications. Paper prepared for the Congressional Research Service by the Lyndon Baines Johnson School of Public Policy at the University of Texas at Austin.

United Nations (2003), World Public Sector Report: eGovernment at the Crossroads, New York: United Nations.

Section 4: Legal Solutions to Barriers to eGovernment

In this section, we propose legal solutions to the remaining barriers to eGovernment within the 8 legal areas identified in the course of the project. The legal areas are:

- Administrative law
- Authentication and identification
- Intellectual Property Rights (IPR)
- Liability
- Privacy and data protection
- Public administration transparency
- Relationships between public administrations, citizens and other ICT actors
- Re-use of public sector information

For each area we provide a brief outline, nominate at least two barriers and propose a solution. As with the organisational solutions we are not aiming to produce solutions to all the potential problems of eGovernment, but to identify a range of tangible solutions to specific key obstacles.

Administrative Law

Dr Julián Valero Torrijos

Department of Administrative Law, University of Murcia, Spain

Introduction

In most EU states, public administrations are governed by a specific form of regulation, known as Administrative Law, which is quite different from regulation that rules the relationships between individuals. However, Administrative Law is not applicable in such an intensive way in those countries (e.g. the UK) that are influenced by the legal Anglo-Saxon model of public administration, which is ruled mainly by common law.

Administrative Law is characterized by the attribution of significant powers to public bodies, together with the recognition of relevant formal guarantees for citizens. The existence of these rules may become an obstacle to the implementation or consolidation of electronic public services. However, if legal adaptations to take account of ePublic Services do not affect Administrative Law by being limited to the general regulation of private individuals, the resultant lack of juridical security for the use of ICT in the relevant administrative activities can become a major barrier to an administration's modernization. An inadequate or non-existent adaptation of Administrative Law to the requirements of technology may also involve a lower level of guarantee for private individuals and companies, which could threaten their essential role as users of eGovernment services.

Bearing in mind the deeper analysis on the implications of eGovernment for Administrative Law examined in Deliverable 1b of this project, this section proposes concrete measures that may be useful in overcoming two of the main barriers: poorly adapted regulations affecting the procedures for taking administrative decisions; and the lack of adaptation of general regulations on ICTs to the specific requirements of eGovernment within the legal framework for public administrations.

Adapting formalized regulation on administrative decision making to enable the full potential of electronic technologies to be realized

The value to eGovernment of simpler and more flexible regulation

One of the main goals of Administrative Law is to ensure that decisions made by public administrations are adopted through the appropriate procedure. Decisions passed without respecting this formal requirement can be considered invalid. This is probably the most representative characteristic of Administrative Law, since it is an essential tool in controlling the correct formation of administrative decisions, both in terms of legality and opportunity. Such a procedure is important since, except in some very rare and isolated cases, all decisions with legal implications must respect this requirement.

Introducing simpler and more flexible regulation relating to ICT - enabled public administration activities is of growing value because many public services and administrative activities can now be carried out more effectively and efficiently through electronic media. This kind of adaptation should not imply a decrease in regulatory guarantees, but only be an adaptation to accommodate electronic media.

A higher level of streamlining and flexibility of rules and procedures than for traditional methods is required for implementing eGovernment services in order to take account of specific ICT capabilities, such as sharing information across organizational, administrative and juridical borders. This will help to realize the full potential benefits of the use of electronic media in decision making and in establishing effective communication with citizens and companies. Such a simplification is one of the main priorities of citizens in those States with a continental as opposed to Anglo-Saxon model of public administration. For example, according to a survey by BVA[6] in France, 60% of those polled declared such procedural simplification should be the main public administration priority.

Administrative Law adaptations are therefore needed to allow greater flexibility to improve administrative operations and efficiency by carrying out many tasks and processes automatically through eGovernment services. These electronic channels often do not require a formal procedure or follow a more informal process than that fixed for actions carried out using traditional tools based on written documents and personal relationships. If the legal framework does not support particular typical features of eGovernment, then a serious problem for administrative decisions and communications is likely to appear as a result of a conflict between the speed that is allowed by ICT-enabled services and the formal requirements imposed by the traditional regulation of administrative procedures. In this context, it is important to emphasize that the more flexible procedures needed to facilitate eGovernment services do not mean less security in their operation; in practice, the technology's capabilities can even improve security.

Certain Administrative Law requirements may not only hinder the effectiveness of an administrative activity but also become a serious barrier for the general competitiveness of the EU and of Member States' national economies and companies. One of the main objectives of the European Commission's (2006) i2010 eGovernment Action Plan is to reduce administrative burdens by making efficiency and effectiveness a reality with the support of ICTs. This need for eGovernment services to help simplify administrative procedures is recommended by the report on eGovernment in the EU in the Next Decade for the European Commission's Institute for Prospective Technological Studies (Centeno et al. 2004). As a clear example of the possibilities offered by ICT means to streamline administrative procedures, the Dutch Horeca project has offered an integral form with which starting entrepreneurs can apply online at a time for several licenses and dispensations they need, to start up their business[7].

Technological modernization certainly opens opportunities to achieve this goal. There is a serious risk, however, that administrative activity will continue to be carried out using the traditional underlying processes – even though the tools employed may change, from paper to digital. Any project on eGovernment must therefore take account of the ways in which electronic services offer a unique opportunity to simplify administrative procedures, especially in terms of data input by users and in the amount and kind of documentation that needs to be provided. An eGovernment innovation also creates a space for re-analyzing formalities that have previously applied, but need to be changed or completely eliminated when moving to electronic media. For instance, the Danish Commerce and Companies Agency (2005) has noted that most of the legal hindrances to eGovernment it identified had come from formal requirements.

Developing appropriate policies at different levels

The issues outlined above are particularly relevant at the national level, and some Member States have indeed tried to solve this challenge of simplification. The French eGovernment's Strategic Plan[8], for example, has a main aim of promoting the evolution of law aimed at removing regulatory obstacles to the development of eGovernment and establishing an overall and coherent legal framework that permits the development of ePublic Services. Other relevant initiatives in this area include the European consultation on 'cutting red tape' (European Commission 2007) and projects to reduce 'administrative burdens' in several Member States, including Sweden[9], the Netherlands[10] or Denmark[11]. The Spanish Law on Electronic Access to Public Services of 22 June 2007[12] has recognized a citizen's right not to

[6] See: http://www.bva.fr and, more generally on this issue, *eGovernment News* (2005).

[7] As a result of its innovative perspective, this project has won an eEurope Award in 2007. For further details, see http://www.epractice.eu/cases/horeca1

[8] See: http://europa.eu.int/idabc/en/document/1351/395

[9] See: http://europa.eu.int/idabc/en/document/4362/330

[10] See: http://www.administratievelasten.nl

[11] See: http://www.amvab.dk

[12] See: http://www.boe.es/boe/dias/2007/06/23/pdfs/A27138-27140.pdf

present certain administrative documents in paper form. Consequently, it obliges public administrations to share the information concerned through electronic means when citizens have given their consent or a legal authorization has been established.

This is a problem that must be solved mainly by national, regional and local authorities, the EU should bear in mind the potential inconveniences and constraints in relation to its own administrative procedures. Strong guidelines for Member States should also be established at the European level to take account of the serious risk of damaging administrative effectiveness and efficiency by a failure to adequately adapt formal Administrative Law regulations. The flexibility made possible by such suitable adaptations is necessary to meet relevant budgetary requirements by ensuring technological modernization achieves its optimum impact. This should be achieved from both the external perspective of relationships with citizens and the internal one of improving the procedures necessary to take quicker administrative decisions based on completely full, accurate and up-to-date information.

The necessary adaptation of the legal framework concerning the administrative formal procedures outlined here is a challenge that must be met primarily by Member States, particularly the authorities at national, regional and local level with competence to modify paper-based rules.

In addition, the EU should stress the importance of taking into account this kind of requirement in relation to eGovernment, particularly in official information highlighting the opportunities opened by ICT-enabled capabilities to improve public administration efficiency and effectiveness. eGovernment projects do not always focus sufficiently on this perspective and on the deep transformation in administrative and organizational structures and processes enabled by the technology. More formal encouragement from the EU level to prioritize these aspects could raise awareness of their significance among public administrations.

Recommended solutions

The above analysis leads us to make the following proposals to Member States and the European Commission:

- draw up a complete catalogue of all the administrative procedures within the competence of the concerned public administration;
- analyze all existing formalities and documents required by citizens and businesses, with the aim of redesigning any where changes are needed to meet the special characteristics of ICT-based applications to eGovernment;
- eliminate all formalities associated with the traditional approaches being phased out (e.g. documents unnecessary to carry out a specific task), and substitute them with only those administrative documents required by citizens for their online data interchanges with public administrations;
- as a consequence, recognize a citizens' right not to have to present again those documents that are already held by a public administration.

The effectiveness of these recommendations will depend on the approach taken by the public authorities in charge of related eGovernment initiatives adopting this perspective. To ensure these are well implemented, at a national level there should be a legal requirement for any decision about further developing eGovernment procedures to be preceded by actions that fulfill the above recommendations.

Possible indirect effects on other barriers and obstacles of these measures should also be taken into account. For instance, online data interchanges must be designed with a strict respect to relevant data protection rules (see also Section 5 of this section on Privacy and Data Protection). And there is a strong need for close coordination between public administrations to establish common technical and organizational mechanisms to facilitate those data transfers. In addition, the requirements of public administration transparency (see Section 6) and re-use of public sector information (Section 8) may also be affected, since traditional paper-based rules are not always conceived from a perspective as open as that made possible by electronic media. A special effort should therefore be made to overcome any limitations and exceptions that are not sufficiently justified.

Revising general regulations on ICTs to meet specific needs of eGovernment (e.g. on liability) within the legal framework for public administrations

Most EU Directives and other rules – particularly those passed at the national level by Member States in transposing Directives – regard issues related to electronic technologies as being conceived mainly to guarantee and protect the existence of a European internal market. These regulations and rules are therefore usually addressed at establishing a legal framework suitable to assure the free movement of goods and services. Public administrations, however, are generally not engaged in activities of an economic nature. When passing regulations in this field, public administrations are therefore considered only as actors who must guarantee the compliance of their provisions, rather than as a specific group being addressed by a provision.

Liability and the hosting of ePublic Services

As public bodies in countries adopting Administrative Law are governed by different rules to those applicable to private relationships, it is often not clear which rules must be applied in the public sphere and what happens if there is a contradiction between the implications for public and private contexts. This is illustrated in the field of liability by Directive 2000/31/EC on data retention and Directive 2006/24/EC (as amended by Directive 2002/58/EC) relating to public bodies acting as intermediaries. These are particularly relevant in the field of eGovernment because they include specific rules that taking account of the unique aspects of electronic services. However, they do not enable a clear response to key questions to be given in certain circumstances.

The following examples relating to liability issues and the hosting by larger public authorities of ePublic Services can help to illustrate the relevance to eGovernment of the lack of appropriate and clear adaptation of Administrative Law. They also highlight the singularities of public administration requirements in this field, particularly in terms of the administration's own legal framework when adopting a regulation or formal document relating to ICTs. The examples show why it is important to explicitly clarify whether or not rules are to be applied to the activities of public administrations.

One example relating to the question of liability indicates the particular need for clarification in situations where one organization hosts the services run by another. In eGovernment, this is typified by the hosting by a regional administration of an ePublic Service on behalf of a local administration. Certain local public administrations, particularly those municipalities with smaller populations and/or more limited resources, are not able to offer electronic public services unless other administrations cooperate with them to provide both advice and technical support. For this purpose, regional or provincial authorities may supply hosting services for the applications and information systems required to offer the necessary local eGovernment services. However, it needs to be made clear whether or not the administration hosting the Website will also be responsible for any damage caused by the information offered.

As the European Commission (2006) has acknowledged, one of the main challenges of inclusive electronic public services is to endeavour to close the digital divides in order to ensure by 2010 that all citizens become major beneficiaries of eGovernment. Uncertainties cause by this kind of legal doubt could increase the risk that many of those living in smaller or less well resourced municipalities will not be able to become users of electronic services.

From a different but complementary perspective, some local authorities have decided to promote the use of the Internet and access to ePublic Services through public 'points of access'. This seeks to avoid leaving certain groups of citizens behind, as recommended by the European Commission's (2006) Action Plan. These kinds of initiatives help to address digital divides because they are essential not only in certain rural areas or remote geographical locations, but also in assisting to incorporate various disadvantaged social groups into the Information Society.

In the provision of such access points, public administrations act as Internet Services Providers (ISPs), but without the commercial purpose that characterizes other ISPs. It is then not clear whether the liability limitations established for intermediaries can be applied to public administration activities. This has important consequences because many Member States have a different and more severe liability system for public administrations compared to the private sector.

Clarifying the scope of regulations

In addition to the uncertainties about the legal framework concerning liability, there are legal doubts in other areas such as data protection. For instance, a question is raised about whether or not public administrations must be considered, as specified in Article 1 of Directive 2006/24/EC, as “providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime”.

However, public administrations do not supply services in the strict sense used by European Law. Article 2 of Directive 2000/31/CE, for example, states that the concept of ‘service’ must be understood within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC. The preamble to the latter states (in Section 19) that “services” means those normally provided for remuneration. Yet this characteristic is absent in activities that a State carries out without economic consideration in the context of its duties, in particular in the social, cultural, educational and judicial fields. This raises the question of whether or not public administrations provide “services” and, therefore, if they are obliged to retain the traffic data related to their services.

Member States should clarify the scope of the regulations they pass in transposing Directives to their national laws. Nevertheless, this process of adaptation in European Law does not always take into account the singularities of an internal legal framework, particularly when a clear exception or authorization for the public sector is not fixed in a Directive, in the way that exceptions are made in Directive 95/46/EC on data protection.

As the main aim of this Directive is to establish regulation mainly for private services suppliers and not to rule on the activities of public administrations, Member States may extend their own legal provisions to public administrations as there is no prohibition on this at the European level. Nevertheless, the regulation regarding these issues contained in subsequent related Directives do not contain explicit references to these exceptions. This produces a serious risk of juridical insecurity, particularly in the field of data retention, since the serious crimes (e.g. terrorism) referred to by Directive 2006/24/EC on data retention can also be committed using services provided by public administrations.

On the other hand, the limitations of liability established by Directive 2000/31/EC (in Article 12 and, particularly, Article 14) refer to the activity of ICT intermediaries but do not make clear whether public administrations may be considered as one of these. If such rules are not applied to the activities of hosting or access supplied by them, these bodies could be responsible for the damages caused by a third party, even if they do not have an active role during the transmission of information or actual knowledge of illegal activities or information.

Recommended solutions

We therefore recommend to Member States that they extend their regulation on liability and other hosting - related issues to public administrations. In addition, we suggest that the European Commission should either:

- clarify, through a formal document, the scope of Directives 2000/31/EC, 2002/58/EC and Directive 2006/24/EC; or

- introduce a binding measure on Member States to promote a higher level of harmonization and juridical security, including modifications to include public administrations among those addressed by this kind of regulation.

References

Publications

Centeno, C., van Bavel, R. and Burgelman, J - C. (2004), eGovernment in the EU in the Next Decade: The Vision and Key Challenges, Technical Report EUR 21376, Brussels: Institute for Prospective Technological Studies (IPTS), European Commission, http://europa.eu.int/idabc/servlets/Doc?id=19131

Danish Commerce and Companies Agency (2005), Better eGovernance. A Measure of eGovernance in New Danish Laws, http://ec.europa.eu/idabc/en/document/4295/333

eGovernment News (2005), French Government Unveils New State Reform Plans, eGovernment News, 29 July, http://europa.eu.int/idabc/en/document/4501/194

European Commission (2006), i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, Brussels: European Commission, http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/egov_action_plan_en.pdf

European Commission (2007), Action Programme for Reducing Administrative Burdens in the European Union, Communication from the Commission, COM(2007)23, Brussels: European Commission, http://ec.europa.eu/enterprise/regulation/better_regulation/docs/com_2007_23_en.pdf

EU - level, national and other relevant legislation and regulations

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281, 23/11/1995, pp. 31 - 50, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (the updated status of implementation is at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm).

Directive 98/34/EC of 22 June 1998 on laying down a procedure for the provision of information in the field of technical standards and regulations, Official Journal of the European Communities L 204, 21/7/1998, pp. 37–48, http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_204/l_20419980721en00370048.pdf

Directive 98/48/EC of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, Official Journal of the European Communities, L217, 5/8/1998, pp. 18–26, http://ec.europa.eu/enterprise/tris/98_48_EC/index_en.pdf

Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the European Communities L 178, 17/07/2000, pp. 1-15, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal of the European Communities L 201, 31/07/2002, pp. 37-47 ('Directive on privacy and electronic communications'), http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Communities L 105, 13/4/2006, pp. 54–63, http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf

Authentication and Identification

Dr Sjaak Nouwt

Tilburg Institute for Law, Technology and Society (TILT), University of Tilburg, Netherlands

Introduction

Authentication in an eGovernment context is typically an act of establishing or confirming someone or something as authentic, involving any process through which one proves and verifies certain related information. Electronic authentication provides a level of assurance as to whether someone or something is who or what it claims to be in a digital environment.[13] Identification is an act of establishing or confirming the identity of a person. Identification is the process of uniquely differentiating a person (or a thing) from all other persons (or things).[14]

The seven barriers that have been identified in this project (see section 2) can all be related to this subject. However, two are of particular overall significance with regard to authentication and identification: poor coordination and lack of trust. Poor technical design is also a significant barrier here, but for practical reasons such design issues are best considered as being closely related to a lack of trust when considering solutions for this legal area. The following recommendations therefore focus on the coordination and trust barriers to eGovernment. The solutions suggested could be considered as a contribution to a possible new EU Directive on eGovernment.

Improving coordination

The paper on Authentication and Identification in Deliverable 1b of this project refers, in the discussion on the ‘poor coordination’ eGovernment barrier category, to a decision by the European Commission (2006a) to continue to encourage the development of eSignature services and applications and to monitor the related market. This places particular emphasis on interoperability[15] and cross border use of electronic signatures.

Apart from eSignature problems caused in Europe by misinterpretations of the eSignature Directive (1999/93/EC) and by divergences in European legislation and the practical application thereof, Dumortier et al. (2003) have identified the lack of interoperability and the increasing use of electronic signatures as big obstacles for the acceptance of eGovernment services. The authors of the European Commission (2006b) report on related eBusiness practices conclude (in Chapter 4.6.4): “cross-border use of electronic signatures depends on the possibility of a party to technically receive, read and control the other party’s electronic signature.”

2.1 Recommended solutions

According to the European Commission’s (2006c) ‘i2010’ eGovernment action plan, “interoperability is a key enabler”. The Commission states that it will aim for better cooperation between Member States through the creation of a work programme between 2006 and 2010 for closer cooperation on the management and authentication of, and easier cross-border access to, electronic records and archives in public administrations. This was extended and

[13] OECD Recommendation on Electronic Authentication and OECD guidance for Electronic Authentication. June 2007, p. 7. Available at: http://www.oecd.org/dataoecd/32/45/38921342.pdf.

[14] See also Thierry Nabett, Mireille Hildebrandt (eds), Inventory of topics and clusters. FIDIS deliverable D.2.1, version 2.0 (21 September 2005), p. 36. Available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.1_Inventory_of_topics_and_clusters.pdf.

[15] See also the work done by the FIDIS-project on Interoperability (Future of IDentity in the Information Society), available at: http://www.fidis.net/resources/deliverables/interoperability/.

supported by the Lisbon Ministerial Declaration of the 19th of September 2007 where cross-border interoperability was identified as a key priority policy action[16].

Technical and commercial interoperability are important conditions for cross border use of eSignatures. To enhance such uses, additional requirements by the public sector for receiving eSignatures should be kept to a minimum. Furthermore, other EU legislative initiatives could increase the cross border use of eSignatures, as seen in the Procurement Directives (2004/17/EC and 2004/18/EC) and the Invoice Directive (2001/115/EC).

Coordination (e.g. through a standardized system of eSignatures for the public sector) is therefore essential to the promotion of wider use of eSignatures, a key aspect in many eGovernment services. We recommend the following legislative changes to help achieve this:

- Keep to minimum additional requirements by the public sector for receiving eSignatures (see Article 3.7 of Directive 1999/93).

- To promote interoperability and the cross border use of eSignatures, Member States should be obliged to notify a European standardization organization, like the European Telecommunications Standards Institute (ETSI) or the European Committee for Standardization (CEN), about national standardization initiatives with regard to eSignatures. Notifying the ETSI or CEN could assist to promote the use of interoperability standards for the technical implications of Annex I of Directive 1999/93/EC, as recommended in the Dumortier (2003: p. 6.) report. This should also make it easier for cross-border workers and inhabitants of border areas to use an eSignature for accessing records in the (other) country where they work or live.

- The EU should prescribe by legislation that eSignatures used in the public sector should comply with a certain standard. This can be a national standard, with the ETSI or CEN controlling the adequate level of standardization of Member States' national standardization initiatives. The ETSI or CEN could also take the initiative to develop a European standard for eSignatures in the public sector, based on the national initiatives. In this respect, the EU could also require Member States to cooperate.

- The EU should require Member States to mutually recognize the eSignature standards developed in other Member States, when these are approved by the ETSI or CEN. This legislative change could be achieved by amending the eSignatures Directive 1999/93/EC (see European Commission 2006a).

These changes could contribute to achieving the broader aim of addressing the coordination barrier to eGovernment, perhaps through a European eGovernment Directive that would include interoperability regulations and other issues concerned with authentication and identification mechanisms.

Such an eGovernment Directive could take as an example existing legislation outside the EU. For instance, the US eGovernment Act of 2002 (PL 107-347), which furthered the push provided by the Government Paperwork Elimination Act of 1998, includes provisions for the interoperability of related solutions across agency boundaries (Holden and Millet 2005). Federal agencies must ensure that electronic signature implementations are consistent with the policies of the Office of Management and Budget (OMB) that stress government-wide solutions. For example, the Act designates the General Services Administration as the federal agency leading efforts to create a framework for eSignature interoperability.[17]

It must be noted that we realize that standardization efforts have already been made, e.g. by the European Electronic Signatures Standardization Institute (EESSI), "to co-ordinate the standardization activity in support to the implementation of Directive 1999/93/EC on electronic signature".[18] However, the ICT Standards Board decided to close the EESSI Working Group

[16] Ministerial Declaration approved unanimously at the 4th Ministerial eGovernment Conference in Lisbon, Portugal. http://www.epractice.eu/document/3928

[17] In this respect, reference can also be made to the Summary Report (Majava and Meyvis 2007) on an IDABC interoperability workshop on electronic Identity Management (eIDM), which aimed "to address ID related standards" (p. 5).

[18] See the website of EESSI: http://www.ictsb.org/EESSI_home.htm.

in October 2004. The standardization work is continued by ETSI TC/ESI, where standardization in the area of electronic signatures and infrastructures is currently taking place.[19]

Lessons can be learned from innovative countries in the field of authentication and identification for eGovernment, such as New Zealand, or Austria. However, the federal organization of the United States of America seems to be better comparable with the EU than a country like e.g. New Zealand.[20]

The importance of standardization has been confirmed by two members of the expert group of this project, whom we consulted for this solutions chapter. We realize that our recommendation for standardization can best be considered applicable to different levels: technical, legal, and socio-cultural or organizational. Standardization at all these levels may not be easy to achieve and it also may not be easy to achieve standardization of authentication and identification procedures for life time events. Therefore, one could focus to limit standardization to sectoral applications instead of government services as a whole. The mutual recognition of eSignatures, or authentication and identification procedures in general, could also be considered as an alternative when it would appear that standardization is impossible.

Building trust in eGovernment

A lack of trust is quite common when someone has to use electronic means to achieve a goal. Most people are still accustomed to using paper and a pen to establish certain agreements, particularly those requiring a signature. Many people also still rely more on paper-based data than electronic data. There are some good reasons for this, as the use of computers and the Internet still has flaws. Accidents and system problems happen, as with failures in the immigration and Child Support Agency computer services in the UK (Dutton et al. 2005: p. 14). Furthermore, there are strong implications for the surveillance of citizens. In countries such as the Netherlands and US, computer experts and civil liberty groups have also criticized the use of voting machines in elections as they can be considered to be ‘black boxes’ that cannot provide a clear audit trail or strict safeguards against fraud (Dutton et al. 2005: p. 13).

These kinds of problems undermine trust in eGovernment. However, trust in government is different from trust within private organizations (Holden and Millet 2005: p. 368):

- many of the transactions individuals undertake with government are mandatory, whereas they are often entered into out of choice in the private sector;
- because of the heterogeneity of citizens, government agencies face a very diverse user population with different levels of education and skills training, cultural perceptions, language understanding, etc.;
- some relationships between government and citizens are long term, even from cradle-to-grave, while others involve contacts at intervals, thus creating challenges for authentication and identification mechanisms;
- as a result, citizens may expect more precautions from government agencies than from the private sector in protecting the security and privacy of personal data.

Citizens therefore expect especially high trustworthiness for government management of personal information to prevent unauthorized or accidental disclosure of the highly sensitive personal information held by many public agencies (Holden and Millet 2005: p. 368). But trust in eGovernment involves more than only trust in the fair use of personal information, as it also has to do with uncertainty (Dutton et al 2005: p. 15). For example, uncertainty can exist about the functioning of the Internet, including trust in the technology and in the Internet Service

[19] Technical Committee on Electronic Signatures and Infrastructures of the European Telecommunications Standards Institute: http://portal.etsi.org/esi/el-sign.asp.

[20] See for example the All-of-government Authentication Programme of New Zealand: http://www.e.govt.nz/services/authentication/.

Provider (we could call this ‘the first trust game’). In addition, there can be uncertainty about the people who use the Internet for the provision of a government service (we could call this ‘the second trust game’). Of course, here we are dealing with the second trust game.

The US eGovernment Act of 2002 mentioned in the previous section as a possible aid to improve eGovernment coordination also seeks to promote trust in eGovernment. It does this by obliging federal agencies to conduct Privacy Impact Assessments (PIAs) for new electronic information systems and information collections that involve the use of personally identifiable information (Holden and Millet 2005: p. 371). These agencies must share the response to a series of questions with the OMB when requesting funding for a new system, with results of responses made public. This Act also requires the posting of privacy notices, which advises users of the information practices adhered to by a website.

These privacy-related issues are important for authentication and identification in eGovernment, particularly as government plays a dual role in authentication. Firstly, it is an organization that issues identity credentials[21] to individuals and validates those credentials when presented by a user attempting to access a protected Web resource. Secondly, it is also a party relying on the authentication of someone's identity as represented by their credentials, when that party is in communication with a government section. As the issuer of identity credentials, the government is not an independent authority. The government is judge and jury at the same time. As a result, this dual role for government could contribute to the undermining of trust in eGovernment.

Recommended solutions

Inter-agency eAuthentication solutions are likely to have significant privacy implications because of their facility to link databases and create electronic dossiers. Therefore, a solution that is secure, usable and still sensitive to privacy concerns is crucial, but seems difficult to find (Holden and Millet 2005: p. 372).

Transparency, privacy, security, identity and trust are related topics. This is recognized by Dutton et al (2005) in their development of trust-enhancing strategies for eGovernment. We recommend that the European Commission considers the range of issues identified in these strategies in developing its legislation related to eGovernment, such as to:

- enable citizens to gain experience with the use of Internet and, thereby, learn to use it in a safe way;
- manage the trust tension between citizens’ concerns about privacy, security and identity and their obligation to provide personal information to receive the benefits of eGovernment services, especially by using low trust applications where possible[22];
- establish agreements, guidelines and frameworks to enhance trust;
- use Privacy Enhancing Technologies (PETs) to boost trust (see also Section 5 of this chapter);
- design, build, run and evolve sustainable ICT systems.

We would like to add to this list that government agencies in the member states should be obliged to conduct Privacy Impact Assessments (PIAs) for new electronic information systems and information collections that involve the use of personally identifiable information.

Other existing legislation, such as the US eGovernment Act, could again serve as examples to help overcome this barrier. Establishing a European eGovernment Directive bearing in

[21] Government is an issuer of identity credentials as it is the certifier for public authorisation keys. The eSignature Directive (1999/93/EC) uses the term “certification-service-provider” for the certification issuer, which is defined as an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

[22] See also section 3 of this report where “low trust applications” are described as applications with low authentication and identification requirements.

mind these recommendations for legal measures and certain guarantees for the citizen could be a sound foundation for building better trust in eGovernment services.

Other solutions in this section, such as those for Privacy and Data Projection and Public Administration Transparency can also help to build trust in eGovernment.

References

Publications

Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., Van Eecke, P. (2003), The Legal and Market Aspects of Electronic Signatures. Legal and Market Aspects of the Application of Directive 1999/93/EC and Practical Applications of Electronic Signatures in the Member States, the EEA, the Candidate and the Accession Countries, Leuven: ICRI, http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

Dutton, W. H., Guerra, G. A., Zizzo, D. J. and Peltu, M. (2005), The Cyber Trust Tension in e-Government: Balancing Identity, Privacy, Security. Information Polity 10, 13–23, p. 15.

European Commission (2006a), Report on the Operation of Directive 1999/93/EC on a Community Framework for Electronic Signatures, COM (2006) 120 final, Brussels: European Commission, 15 March, Brussels: European Commission, http://europa.eu.int/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf

European Commission (2006b), Benchmarking of Existing National Legal e-Business Practices, From the Point of View of Enterprises (e-Signature, e-Invoicing and e-Contracts), Draft Final Report, November, Brussels: European Commission, Directorate-General for Enterprise and Industry, http://ec.europa.eu/enterprise/ict/policy/legal/2006-bm-cr/ramboll-benchmarking-final-report-draft.pdf

European Commission (2006c), i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, EC COM (2006) 173 final, Brussels: European Commission 25 April, http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm).

European Ministers (2007), Ministerial Declaration approved unanimously at the 4th Ministerial eGovernment Conference in Lisbon, Portugal, http://www.epractice.eu/document/3928.

Holden, S. H. and Millet, L. I. (2005), Authentication, Privacy, and the Federal eGovernment. The Information Society, 21: 367–77.

Majava, J. and Meyvis, E. (2007), eID Interoperability for PEGS - Summary Report of IDABC eIDM interoperability workshop, 10 May, Brussels: European Communities 2007, http://ec.europa.eu/idabc/servlets/Doc?id=29055

Nabett, Thierry, Mireille Hildebrandt (eds) (2005), Inventory of topics and clusters. FIDIS deliverable D.2.1, version 2.0 (21 September 2005), http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.1_Inventory_of_topics_and_clusters.pdf.

EU-level, national and other relevant legislation and regulations

Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities L 13, 19/01/ 2000, pp. 12-20, http://europa.eu.int/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf

Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax, Official Journal of the European Communities L 15, 17/01/2002, pp. 24–8, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=32001L0115&model=guichett&lg=en.

Directive 2004/17/EC of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors, Official Journal of the European Union, L 134, 30/4/2001, pp. 1-113, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

Directive 2004/18/EC of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, Official Journal of the European Union, L 134, 30/4/2001, pp. 114-240, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en01140240.pdf

OECD (2007), OECD Recommendation on Electronic Authentication and OECD guidance for Electronic Authentication. June 2007, http://www.oecd.org/dataoecd/32/45/38921342.pdf

Intellectual Property Rights

Dr Maurice Schellekens

Tilburg Institute for Law, Technology and Society (TILT), University of Tilburg, Netherlands

Introduction

eGovernment is enabled by the use of ICTs. Both the information disseminated and the supporting technology employed are subject to Intellectual Property Rights (IPR), such as copyright, trademark rights or patents. If the public body involved in eGovernment initiatives is not the 'rightsholder' who owns the IPR, licences must be arranged to enable the relevant information and ICTs to be used appropriately.

Solutions are recommended in this section to two main barriers that can arise in eGovernment from IPR-related issues: obstacles posed by the costs of accessing IPR material; and problems of trust in relation to essential software needed for eGovernment services, especially for open source software.

Addressing the potentially high costs of access to IPR protected material

Concerns about the costs to eGovernment users of being allowed access to IPR-protected information, services and products need to be understood and dealt with in a way that balances the requirements of the rightsholder, the user and the government body wishing to provide an ePublic Service.

In the course of their activities, public administrations often have to present information for which it does not own the rights. For instance, when granting a building permit, the relevant government agency may have to exhibit certain information, such as an architect's drawing of the building for which a permit has been requested or granted. This requires the consent of the architect who is the rightsholder to the drawing, typically in the form of a licence.

When moving to eGovernment services, a public agency may want to place such an architect's drawing on its Website. In terms of copyright law, this presentation in digital form is an independent act, distinct from traditional physical exhibition. As this therefore requires a separate consent, public bodies need to adapt licences relating to eGovernment in order to gain the consent for Internet use of such third-party information. Failure to clear rights to the information and technology used in eGovernment services constitute an infringement to the pertinent IPRs. An accusation of infringement can lead to a disruption of an eGovernment service because an IPR rightsholder can refuse a licence, without having to give a justification for the refusal.

Generally, a rightsholder does not have an interest in disrupting eGovernment services. However the threat of taking such action places the rightsholder in a strong bargaining position. This opens possibilities for rightsholders to extract high licence fees from the governmental body.

One clear solution to this problem is for the government body to negotiate the licence at an early stage, preferably when commissioning the work required. At that stage, the rightsholder is in a relatively weak position of still having to compete with other companies or professionals for the work. This should help to make the rightsholder more likely to be willing to agree a licence at a reasonable price to allow the future Internet use of whatever has IPR protection.

However, there are many situations in which this solution does not work. For instance, many works made available to the public by a government body may have not been commissioned by that body (e.g. a person seeking to obtain a building permit who commissions the drawings to be used in the application from an architect, not the public body). There are also many existing works predating the era of eGovernment, for which an 'Internet licence' has never been solicited. These pose difficulties for government because each of the rightsholders with which the public body has to negotiate has the power to refuse a licence. In cases where certain rights are essential to make an eGovernment service work, the refusal of any of the rightsholders may make the proposed eGovernment service unfeasible.

Any government body can be confronted with this problem, since the basic law on IPR is highly harmonized in the EU (e.g. see the many Directives about IPRs mentioned in Deliverable 1b of this project, such as Directives 96/9/EC and 2001/29/EC discussed below). However, some countries have exceptions in their copyright laws that make it easier for government bodies to deal with these situations (e.g. Article 15b of the Dutch Copyright Act). In addition, the use of third-party works by governmental bodies has not yet been harmonized.

Recommended solutions

In each Member State, rightsholders should be subjected to the same rules concerning government use of their works. However, the lack of harmonization regarding use of third-party works by governmental bodies is being felt increasingly as eGovernment services gain momentum.

Directive 2001/29/EC on the harmonization of copyright and related rights mentions a number of exceptions to the exclusive rights of the holder of a copyright. Member States have the option to decide whether or not to include these exceptions in their national laws. The limitation of copyright most relevant in the context of eGovernment is contained in Article 5(3e) of the Directive, namely the exceptions relating to: “use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings”.

For eGovernment purposes, the element of the proper performance of administrative proceedings is the most relevant. A varied picture emerges when assessing how this element has been implemented in various Member States (see Westkamp 2007). In some Member States, no or a severely restricted exception for administrative proceedings exists. In Belgium, the exception is limited to databases; in Estonia and Greece, there is no exception to the right to ‘make available’[23] a work; in Latvia, there is no exception for administrative proceedings; the Slovak republic does not have an exception in the field of art. 5(3)(e) whatsoever. In a number of other Member States, the limitation for administrative proceedings is subject to qualifications. That makes it cumbersome to find out whether a cross border service can rely on an exception for administrative proceedings. These countries include: Finland (focus on public statements and obtaining information), Hungary (evidence related), Norway (focus on proceedings and freedom of information act), Sweden (use of statements before authorities) and UK (very extensive and detailed rules in Articles 45–50 of the Copyright, Designs and Patents Act 1988).

In the light of these divergences, it is desirable for a uniform exception for administrative proceedings to be made compulsory in the copyright laws of all Member States. At the same time, regard must be given to Article 5 Section 5 of the Directive. This explains that the exceptions and limitations it specifies shall be applied only “in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests” of the rightsholder.

This provision implies that it is necessary to allow these exceptions only on the condition that rightsholders receive a fair compensation for the use of their works. The end result of this process will be that the bargaining position of the rightsholders is reduced, as they will no longer be able to refuse licences. The only question then to be answered is the level of the licence fee. If a governmental body and a rightsholder cannot agree on a fee, it is ultimately a court of law that determines what fee constitutes a fair compensation for the rightsholder.

[23] A copyright is a bundle of rights, including inter alia the reproduction right; the right to distribute physical copies; the right to broadcast; and the right ‘to make the work available’. When placing works on the Internet, two rights from this bundle are usually relevant: the reproduction right (because placing a work on a web server involves copying the work) and the right to make the work available (because placement on a web server makes the work accessible to anybody).

The same solution could be considered for the rights in databases, on the basis of Directive 96/9/EC on the legal protection of databases. Article 9 of this Directive offers the following optional exception to the 'sui generis'[24] database right: "Member States may stipulate that lawful users of a database which is made available to the public in whatever manner may, without the authorization of its maker, extract or re-utilize a substantial part of its contents…" including, among others, "the case of extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure".

However, the future of Directive 96/9/EC is most uncertain following the European Commission's (2005) first evaluation of it, in December 2005. The policy options identified even included the possibility of repealing the entire Directive[25]. Therefore, it is probably not worthwhile to aim at changing the directive before a decision has been made about the directive's future.

Building trust in open source software as an alternative to proprietary products

The functioning of eGovernment depends on the software that runs ICT hardware. There are two main channels for obtaining such software. One is to buy commercial proprietary software for which the supplier holds all rights and retains the 'source code' containing the detailed instructions of the underlying program. The other approach is the use of 'open source'[26] software. In contrast to proprietary software, the rightsholders of open source software allow all modifications to their program and deliver that software with its source code.

The source code is important because it is an essential tool for adapting software when new functionalities are required (e.g. to accommodate changing organizational needs of the government body or when taking on new tasks, as is frequently the case in eGovernment). Access to the source code is also necessary for making software interoperable with other computer programs. The cooperation of the provider holding the software and source code rights is crucial to enabling such modifications, especially when undertaking new eGovernment initiatives where existing software needs to be adapted or is to be made interoperable with new software (e.g. coupling an existing internal database with a web-based application to disclose its contents to the public).

Software that is not standardized can give rise to particular dependence on the provider. Given the dynamic character of eGovernment, such dependence on proprietary software can therefore be felt as a burden. That is why open source can be seen as an attractive option. However, open source software is not without its risks, especially when proprietary and open source software providers compete with each other. The open source solution can then become the target of legal action, such as through an allegation that the open source software infringes proprietary trade secrets, software copyrights or software patents[27].

For public bodies, an accusation of infringement may mean that eGovernment services have to be suspended until all legal issues have been cleared. If the body has made such client software (e.g. a web browser) available to the users of its services, they may have to be given notice that they are using allegedly illegal software. Apart from the cost of putting everything right, such a course of action undermines trust in eGovernment services among users and should be avoided where possible.

Sometimes it is claimed that OSS is more vulnerable to claims of IPR infringement than proprietary software. The idea is that the availability of the source code makes it easier to find infringing lines of code. This raises the question whether the (possible) tension between

[24] The sui generis right is a specific property right for databases that is unrelated to other forms of protection, such as copyright.

[25] For a timeline of events surrounding the future of Directive 96/9/EC, see http://ec.europa.eu/internal_market/copyright/prot-databases/prot-databases_en.htm

[26] For more on open source software, see for example OSSOS (2004) and the MODINIS initiative 'Free/Libre/Open Source Software' (http://www.flossworld.org).

[27] An example of such a battle, but not in the field of eGovernment, was a dispute between SCO and IBM in the US (see: http://www.groklaw.net/article.php?story=2006100901243713).

OSS's relevance for eGovernment and its vulnerability to claims of infringement could be resolved by creating a copyright and patent exemption for OSS? We do however find that OSS developers must stay clear from protected materials, just like proprietary developers of software. That infringements can be more easily discovered in OSS is something that is being said often, but has hitherto never been proven. An IPR exemption for OSS is therefore in our view not needed.

Recommended solutions

Open source should be an option for government, but policy should not force any technological solution. To enable open source to be a viable option, the software problems outlined above should be addressed at all levels, from local to the pan European level. Nevertheless, they are likely to be more relevant where there is greater use of open source programs because legal action by proprietary software providers against open source rivals is most worthwhile where a sizeable market can be captured. This would place the problem more at the national or European level, rather than locally. The legal solution we propose below needs to be implemented by all governmental bodies involved in the choice of software for eGovernment purposes. Instigating the solution at EU level would yield special 'economy of scale' benefits.

This solution is formulated as a recommendation to Member States. It asks them to encourage their government bodies to take account of the following when choosing software essential for the functioning of eGovernment:

1. A government body using open source software developed by someone else should, where possible, negotiate an indemnification from the provider that guarantees the software does not infringe the rights of third parties. As a minimum, the government body should check that the provider has measures in place to prevent third party software from entering the code of the open source program.[28]
2. Where open source software is developed in-house by a government body, it should:

- clearly instruct all programmers what kinds of code can, and cannot, be entered into the open source software;
- ensure that the rights in the code written by its employees are, where necessary,[29] transferred or at least licensed to the government body; and
- have a procedure in place for quickly dealing with notifications that infringing code is present in the open source program.

The above measures may be able to reduce the risk of 'foreign' code to an acceptable level, but cannot completely eliminate that risk.

References

Publications

European Commission (2005), First Evaluation of Directive 96/9/EC on the Legal Protection of Databases, DG Internal Market and Services Working Paper, Brussels: European Commission, http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf

[28] In this respect, see, for example, Article 6 of the European Union Public Licence (EUPL) which contains an indemnification (see http://ec.europa.eu/idabc/servlets/Doc?id=27470). However, vigilance is required because there are many types of open source licence, and sometimes within one project different licences are being used.

[29] This is only an issue if an employment contract explicitly assigns the rights to the employee. See Article 2(3) of Directive 91/250/EC: "Where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the program so created, unless otherwise provided by contract."

Schellekens, M. M. H. (2005), ‘Intellectual Property Issues Relevant for the European Transport Information System’, in Giorgi, L., Klautzer, L., Rahman, A. and Schmidt, M. (eds.), Towards a European Transport Policy Information System, Prague, ETIS-LINK.

Schellekens, M. (2006), ‘Free and Open Source Software: An Answer to Commodification?’, in: Guibault, L. and Hugenholtz, P. B. (eds), The Future of the Public Domain: Identifying the Commons in Information Law, Information Law Series 16, Alphen a/d Rijn: Kluwer Law International, pp. 303–23.

OSSOS (2004), Stichting ICTU, Programma OSSOS (Programme For Open Standards and Open Source Software in Government), http://www.ossos.nl/index.jsp?alias=english

Välimäki, M. (2005), ‘Software Interoperability and Intellectual Property Policy in Europe’, European Review of Political Technologies, 3 December, pp. 1–11, http://www.politech-institute.org/review/articles/VALIMAKI_Mikko_volume_3.pdf

Westkamp, G. (2007), Part II: The Implementation of Directive 2001/29/EC in the Member States, Queen Mary Intellectual Property Research Institute, London: Centre for Commercial Law Studies, Queen Mary, University of London, February http://ec.europa.eu/internal_market/copyright/docs/studies/infosoc-study-annex_en.pdf

EU-level, national and other relevant legislation and regulations

Directive 2001/29/EC of 22 May 2001 of the European Parliament and of the Council on the harmonization of certain aspects of copyright and related rights in the information society, Official Journal of the European Communities L 167, 22/06/2001, pp. 10-9, http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_167/l_16720010622en00100019.pdf

Directive 96/9/EC of 11 March 1996 on the legal protection of databases, Official Journal of the European Communities L 077, 27/03/1996, pp. 20-8, http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31996L0009&model=guichett

Dutch Copyright Act 1912, http://wetten.overheid.nl (in Dutch, look for ‘auteurswet’); http://www.wipo.int/clea/docs_new/en/nl/nl001en.html (in English, not up-to-date).

UK Copyright, Designs and Patents Act 1988, http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

Liability

Dr Maurice Schellekens

Tilburg Institute for Law, Technology and Society (TILT), University of Tilburg, Netherlands

Introduction

eGovernment activities may give rise to damages in certain circumstances. Those who suffer the damages (citizens, businesses and governments) may want to recoup their loss by holding the wrongdoer liable (e.g. a government agency or ICT service or equipment supplier). To avoid this becoming an obstacle to eGovernment, a balance must be found: if victims are not to lose their trust in eGovernment, they must be able to recoup their damages; at the same time, the law must not overshoot the target by making it too easy to hold the wrongdoer liable.

If suing for liability in eGovernment becomes too easy, the law will have a chilling effect on the willingness of those responsible for supplying and supporting public services to engage or participate in eGovernment, thereby slowing down the development and uptake of electronic media by public administrations. Getting the balance wrong may mean that stakeholders hold back from entering the field of eGovernment at all.

This section indicates how such a balance can be found in relation to overcoming two key barriers in this legal area: lack of trust caused by concerns about liability; and fears about potential liability costs.

Ensuring liability does not undermine trust in eGovernment

When some stakeholders in eGovernment can succeed in completely excluding or strongly limiting their own liability, the costs of damages that occur will fall on other stakeholders. There are a number of characteristics of eGovernment that makes the ability to completely exclude liability relatively easy to do in practice. For example, compared to traditional approaches to the delivery of public services: legal relationships in eGovernment are often more complex; the visibility and predictability of risks are more complicated; there is more difficulty in identifying the wrongdoer; tracing malignant third parties who have interfered in the communication or service delivery is harder; proving the relation between conduct and damage is more difficult; and much greater damages can result from the effect of malfunction within the eGovernment process and inaccuracies in the content.

The impact on trust of such difficulties can be illustrated by the example of an eGovernment service offering access to geographical information collected by a public body. A key liability question here could be: If the provider of this service cannot be held liable for errors in the information, what happens when another stakeholder relying on it suffers damages because of errors in the data?

Consider a building constructor who hits a pipeline while digging because the ‘geo’ information fails to depict the pipe. If the constructor cannot hold the information provider liable, and recoup at least part of the costs of the damages caused, he may not use this information service again – or may be willing to pay only a marginal fee for the information because he will have to make extensive checks to verify the correctness and completeness of the information. The constructor’s trust in the eGovernment geo-information service would then have sunk to a low level, or be completely lost.

In general, all stakeholders must maintain a certain basic level of trust for eGovernment to succeed. If only one key stakeholder loses its trust, the ePublic Service can fail. Getting liability wrong could therefore destroy trust, including that which has been painstakingly built in the past. This shows why it is important for all stakeholders to accept a level of liability that is concomitant with their position.

This can again be illustrated by the geo information case. If the information provider accepts some liability for errors in its information, trust with the building constructor will be reinforced.

The risk of being held liable is likely to spur the geo information provider to improve the quality of the information it provides. On the other hand, the knowledge that the information provider will accept some liability lessens the consequences for the building constructor of damages flowing from any errors that may remain. The information will be of more value to the building constructor because he can reduce the costs of checking the information. The geo information provider's interest is in having satisfied customers who will enable the service to be viable in the long run.

Such acceptance of some liability is concomitant with the role of the geo information provider, who is in a far better position than the building constructor to guard the quality of the information – by influencing the conditions under which the information is collected, stored, processed and disseminated. The risk of being held liable if quality is too low also becomes an incentive to ensure quality controls are effective.

The example above is relatively simple in that it is clear which party is liable. In eGovernment this may often not be the case. Many parties are involved: hosting-provider, content-provider, public body, transport provider etc. There is a non-imaginary risk that once damages have occurred and the question of liability is raised, the actors involved will start accusing each other instead of assuming responsibility. Obviously, it is not conducive to trust in eGovernment if victims of a service would get caught up in a web of actors that are only interested in shifting liability to each other. This issue should be addressed up front.

The types of liability dealt with in this section are likely to be most relevant at Member State or regional level. Other eGovernment activities will have a more pan-European character, such as in cross border eProcurement which forms part of priority policy actions identified by the Lisbon Ministerial Declaration of the 19th of September 2007. The project team have also conducted case studies on eProcurement (see Deliverable 2).

Recommended solutions

In the light of the above discussion, the following are key reasons for seeking solutions that involve intervention at the EU level in relation to trust and liability issues:

- Disparities exist between the laws of Member States relating to the liability of government bodies and officials.
- Economic activity is increasingly moving beyond being confined to one Member State, such as through an ePublic Service offered in more than one State (e.g. access to geo information).
- Trust is difficult to split into compartments: a bad experience in Member State X could make a stakeholder cautious in Member State Y, even though Member State Y has its affairs far better regulated.

The solutions at EU and Member State levels recommended here to prevent liability leading to a loss of trust in eGovernment are built around three main observations:

- Trust is subtle. Enacting a law that means a stakeholder cannot escape liability does not necessarily lead to trust among other participants (e.g. the building constructor will lose trust if he has to sue the geo information provider in order to get compensation).
- The disparities between the laws of Member States relating to liability are great (see the discussion of this issue in Deliverable 1b). However, the harmonization of law about liability involves much more than only those aspects affecting eGovernment, which are a small fraction of all liability difficulties caused by these disparities. It is therefore unlikely to be productive, and will perhaps be unwise, to try to harmonize the laws about liability for eGovernment on its own, as this could lead to a further fragmentation of liability as a coherent field of law.
- The European Commission's (2006) i2010 eGovernment Action Plan urges all stakeholders to make efficiency and effectiveness a reality. The Ministerial Declaration at the Conference 'Reaping the Benefits of eGovernment' (2007)

stressed the importance of a reduction of administrative burdens and urged to act upon it with priority.[30]

These observations favour seeking a solution in which public bodies involved in eGovernment services formulate, through open collaboration, what is considered to be best practices in relation to liability and trust in eGovernment. The best practices should take into account solutions 1–7 set out below. If consensus can be reached amongst the public bodies in the Member States, the findings could possibly[31] be laid down in a Commission Recommendation to Member States. The best practices should, particularly, encourage those involved in eGovernment to put appropriate structures in place. These should ensure the undertaking of the following actions by the stakeholders who define the structure of eGovernment infrastructure or services, or who operate the services and so can structurally influence the extent to which events occur that may give rise to liability:

1. Design eGovernment infrastructures and services in such a way that the risk of damages is reduced as much as is economically feasible.
2. Perform an analysis of the remaining risks.
3. Where possible, warn concerned stakeholders of the risks.
4. Build a complaint-handling mechanism that allows for dealing with incidents in an efficient way and has a low threshold of entry, with complaint handling carried out in-house. Where more parties involved in the causation of damage, one public body should cover damages that a citizen suffers even if it is not the party that is liable, thus creating a one-stop-shop for damage redress. Government may later recoup the damages from the actor is ultimately liable.
5. Design a structured process for addressing certain standard incidents that cannot be prevented in an economically feasible way (e.g. for those that occur often, such as errors in geo-maps because of new pipes being laid or other recent changes in the area they depict). An easy and uniform procedure for reporting on such incidents should be defined, including the specification of steps that have to be taken in dealing with a report, and the possible standardization of the amount of damages to be paid in particular circumstances.
6. Open up the option of Alternative Dispute Resolution (ADR) for cases in which the complaint-handling mechanism fails to reach a satisfactory solution and the incident becomes a dispute. Mediation is an example of ADR: a way of dealing with conflict by guiding parties to a solution that they negotiate themselves. ADR is said to be cheaper than dispute resolution in a traditional court of law, with the solutions reached better accepted by the parties than court decisions because the parties themselves positively contributed to the end result reached (e.g. see Rolph et al 1996; Mnookin 1998). In cases of misapplication of Internal Market law by public authorities, citizens and businesses can turn to SOLVIT, a European network of local SOLVIT Centres for out-of-court dispute resolution. Public bodies providing eServices should incorporate a link in their website to SOLVIT.[32]
7. Make available an Online Dispute Resolution (ODR) form of ADR in situations where the relevant parties can gain from not having to convene physically.

The eGovernment barrier relating to trust should be removed if the above actions are taken, as they seek to prevent damages where economically feasible. Since some damages cannot be prevented, parties should be encouraged to communicate about incidents that have given rise to damage and possible liability. This communication can take place through websites, warnings, during complaint handling and, if appropriate, in ADR procedures. Well-structured communication about incidents does more to raise the levels of trust than adequate, harmonized court procedures.

[30] See http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3640, visited December 2007.

[31] This presupposes that a Commission Recommendation does not offend the principle of subsidiarity. Whether or not it does this is still subject to discussion.

[32] See http://ec.europa.eu/solvit/site/index_en.htm visited December 2007.

Overcoming fears and realities relating to liability costs

A potentially significant eGovernment financial obstacle is highlighted by major legal cases in which the plaintiff is awarded a very large amount of liability damages, leaving the defendant financially crippled and perhaps out of business. If such a fate affects a key stakeholder for certain eGovernment services or activities, the continuation of those services or activities would obviously be endangered. However, these kinds of cases are very rare.

A potentially more detrimental effect of liability is the fear that such a dramatic outcome may happen, rather than its actual realization. Stakeholders become hesitant when their anxiety is raised by uncertainty about risks, about the law concerning liability, about disparities between the laws of Member States, or the level of awarded damages. This uncertainty can shift a stakeholder from an open and creative stance to adopting more defensive strategies, thereby failing to use or develop eGovernment to its fullest potential. It can also lead some stakeholders to decide not to undertake certain online activities, or to refrain from setting up ePublic Services at all.

In these ways, the law of liability can have a chilling effect on new eGovernment activities. However, this can be difficult to detect as nobody can see a service that was never set up because the risks were perceived to be too big to take. At the same time, all new initiatives require plans and budgets that need to be approved. If such processes are properly conducted, those providing the investment will call attention to liability risks and will ask questions about how they are being dealt with. The bodies wishing to launch new eGovernment services and activities will therefore need to address the risks associated with liability even if they see no need to do so, in order to provide relevant answers to the initiative’s financial backers.

Addressing the risks will be more difficult, and take up more of the time of those setting up new eGovernment activities, for those services which:

- are novel and thus more difficult to predict;
- take place in contexts where national laws about liability diverge more;
- and are undertaken in circumstance where the level of awarded damages is most uncertain.

The significance of the related concerns depends on the scope of the eGovernment services and activities that are being set up. Where the geographical scope goes beyond the territory of a Member State, the divergence between laws about liability comes into play. The more elaborate an eGovernment service or activity, the more likely is it that associated risks will be more diverse and more difficult to predict. Where the interests at stake are worth more, risks are obviously bigger.

Recommended solutions

The financial obstacle to eGovernment that might be caused by liability concerns is relevant at local, national and European levels. Since the problems encountered at all levels will be similar, it is worthwhile setting out the main lines for solutions at the European level because these must take account of the differences between Member States.

Although at present these differences may be hardly relevant for local and some national initiatives, this may not be the case in the future. Local or national services may grow to become European-wide services, or eventually be incorporated into services with a wider geographical reach. Such growth paths may be easier to establish if, from the outset, risk assessments and general risk management issues have been dealt with in a manner that is at least harmonized, if not completely unified.

The solutions proposed here are founded on two main observations:

- eGovernment involves new services and activities that will give rise to new situations in which damages occur. It may be difficult to predict the risks that materialize; what forms of liability they give rise to; or how related liability law will be applied to the new cases.

- Services have, or will, grow to have a cross border character. This implies that the laws of more than one country are likely to be, or to become, involved.

These observations suggest solutions should, to some extent, be isolated from the specific legal rules on liability applicable in different Member States. As for the above solution relating to trust and liability, this leads to a preference for a solution in which public bodies involved in eGovernment services formulate, through open collaboration, what is to be considered best practices in relation to liability and trust in eGovernment. The best practices should take into account the solutions 1– 3 set out below. If consensus can be reached amongst the public bodies in the Member States, the findings could possibly[33] be laid down in a Commission Recommendation to Member States.

1. Design eGovernment infrastructures and services in such a way that the risk of damages is reduced as much as is economically feasible.
2. Give accurate information about what the service or infrastructure can, and cannot, be used for. There are two reasons for this. Firstly, it avoids costly discussions about the ways in which the services or infrastructures can be used. Secondly, disclaimers are of limited use because the legal effects of liability disclaimers in different Member States diverge. It is better to opt for 'expectation management' (e.g. in the geo information case in the previous section, by having a warning like: 'Our maps cannot be relied upon for digging'). A precise indication of what the infrastructure or services can be used for will mean that damages flowing from their use for purposes other than those originally intended will almost always be at the risk of the users of the service
3. Before engaging in an eGovernment service, representatives of relevant stakeholders should discuss and agree upon the specific liability rules that govern their mutual relations (see Barendrecht et al 2002: p. 174). This means agreement is needed on more specific rules than are available in statutes or case law, in order to tailor the rules to the specific eGovernment activities being addressed. The rules should be laid down in framework contracts that are made public. The reason for this is that statutory or case law often have areas of uncertainty that result in a lack of clarity, especially in relation to a new activity such as eGovernment. When relevant stakeholders agree a way in which these areas of uncertainty are clarified, the parties concerned can seize the initiative. Courts that later have to interpret the law are generally willing to accept the solution the parties have agreed.

References

Barendrecht, J. M., Giesen, I., Schellekens, M. H. M., Scheltema, M. W. (2002), Overheidsaansprakelijkheid voor Informatieverstrekking, Nederlands Recht, Rechtsvergelijking en de Aansprakelijkheid van Particuliere Infomatieverstrekkers, The Hague: BJU.

European Commission (2006), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, i2010 eGovernment Action Plan – Accelerating eGovernment in Europe for the Benefit of All, SEC(2006) 511, COM/2006/0173 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0173:EN:NOT

European Ministers (2007), Ministerial Declaration approved unanimously at the 4th Ministerial eGovernment Conference in Lisbon, Portugal, http://www.epractice.eu/document/3928.

Mnookin, R. H. (1998), Alternative Dispute Resolution, Discussion Paper No. 232, March, Cambridge, MA, Center for Law, Economics and Business, Harvard Law School, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=117252

[33] As indicated in the previous footnote, whether or not a Commission Recommendation such as this offends the principle of subsidiarity is still subject to discussion.

Rolph, E., Moller, E. and Petersen, L. (1996), Escaping the Courthouse: Private Alternative Dispute Resolution in Los Angeles, Journal of Dispute Resolution, pp. 277–323.

Privacy and Data Protection

Professor Cécile De Terwangne and Dr Cristina Dos Santos

Centre de Recherches Informatique et Droit (CRID), University of Namur, Belgium

Introduction

Privacy and data protection are fundamental concerns for most eGovernment services. Related legislation, such as the provisions of the Data Protection Directive (95/46/EC) for the EU, is therefore relevant to all seven barrier categories identified by Deliverable 1b of this project. These concerns relate to legal requirements about all processing of personal data carried by public administrations within Member States (at all institutional levels) and across the EU. They also encompass questions about access to public documents containing personal data made by third parties or other public bodies (which did not originally collect the data), as well as the sharing and re-use of public sector information.

The barriers related to these issues could be increased if the rules protecting personal data are principally applied to prevent or constrain some activities (e.g. in the processing of information about individuals or the transfer of data between public bodies and other entities). In addition to protecting individuals' data protection rights, related legislation should therefore seek to facilitate the free flow of personal data.

As noted in Deliverable 1b, lack of coordination is one of the most potentially significant legal blockages along the Privacy and Data protection dimension. Clear guidance from the 'top' is needed to assist public administrations in assigning relevant responsibilities (e.g. deciding who can access what) and dealing with problems as they arise (e.g. when data is mishandled or errors are created in shared networked services).

Improved coordination is particularly significant at the European level because legislative approaches and solutions developed by the National Supervisory Authorities (NSAs) [34] for data protection and privacy are sometimes different, or even conflicting. This can create significant blockages to the development and use of some eGovernment systems at a pan-European level. A number of initiatives have been established at the European level to help to improve this coordination, such as the establishment of the European Data Protection Supervisor (EDPS)[35] and the Article 29 Working Party[36], which encompasses all NSAs. Nevertheless, much work still remains to be done in this area, as is noted in a Communication from the European Commission (2007a) on better implementation of the Data Protection Directive.

Despite these potential problems, the protection of personal data could and should be compatible with the development of eGovernment applications. To achieve this, an appropriate balance must be maintained between the need to protect individuals' personal data rights and a public administration's requirement to improve the efficiency and quality of its services. In the remainder of this section we will identify solutions to key barriers we identified in Document 1b: overcoming disparities in the implementations of the Data Protection Directive; assessing the value of the use of PINs by public administrations; facilitating the use of PETs; and better balancing interoperability versus data protection requirements.

[34] Provision for these Authorities by Member States is based of Article 28 of Directive 95/46/EC. More analysis on those actors could be found in Deliverable 1b.

[35] The EDPS was established by Article 1(2) of Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies.

[36] The Working Party was set up under Article 29 of Directive 95/46/EC and the relevant tasks laid down in Article 30 of this Directive 95/46/EC and Article 14 of Directive 97/66/EC (see http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm).

Overcoming disparities in implementations of the Data Protection Directive

Disparities between Member States in implementations of Directive 95/46/EC indicate that a diversity of solutions to the same problems and issues have been arrived at by national laws or by NSAs. Examples include the implementation and development of Personal Identification Numbers (PINs) or the application of laws about data protection only to natural persons or to natural and legal persons.

Recommended solutions

Actions could be undertaken at different levels (European, national level) by different actors working in the field of data protection (such as the Article 29 Working Party, or NSAs). Below, we will detail each level of action, as well as the actors involved in each one, to provide clear guidance for the solutions that could be adopted and by whom.

Actions at the European level

Actions by the European Commission

The European Commission has the power to undertake a series of actions to enhance the effective application of the Data Protection Directive as, under the European Treaties, it is responsible for ensuring Community law is correctly applied by States.

The forms such actions should be allowed to take include:

- undertaking an ‘action for non-compliance’ against the Member States concerned to try to bring the infringement to an end.

Where a Member State fails to comply with Community law (whether by action or by omission), the Commission could take whatever action it deems appropriate in response to either a complaint or indications of infringements that it detects itself[37]. Furthermore, anyone may lodge a complaint with the Commission against a Member State about any measure (law, regulation or administrative action), or regarding a practice they consider incompatible with a provision or a principle of Community law.

- if necessary, referring the cases to the European Court of Justice, because of non compliance of national laws with the Directive (e.g. an inappropriate application or appreciation of the requirements of the Directive in concrete cases)[38];
- or/and appealing to the Article 29 Data Protection Working Party to try to harmonize practices and processes, as national Data Protection laws have already been adopted and are in force.

It has recently been announced that the European Commission (2007a: p.2 and comments on pp. 6–8) does not intend to amend Directive 95/46/EC in the near future, as this one “lays down a general legal framework that is substantially appropriate and technologically neutral”. Instead, the Commission will continue to “monitor the implementation of the Directive, work with all stakeholders to further reduce national divergences, and study the need for sector-specific legislation to apply data protection principles to new technologies and to satisfy public security needs”. Such monitoring should contribute to a growing reduction of this barrier in the future.

Furthermore, the European Commission’s future roadmap towards better implementation of the Data Protection Directive aims to pursue “a policy that relies on the future ratification of the EU’s Constitutional Treaty. This seeks to have a significant impact on this field by creating

[37] See Article 226 and following of the EC Treaty.

[38] This approach has been chosen by the Commission in the past with regard to Member States that had not properly implemented Directive 95/46/EC. It is also likely to be the way chosen in the future (see European Commission 2007a: p.6 and p.9), which should encourage national legislators to pursue the proper implementation of the Directive by amendments to the legislations yet in force.

a specific and self-standing legal basis for the EU to legislate on this matter. The Treaty would enshrine (in Article II-68) the right to protection of personal data, with the present division into 'pillars' and the limitations of Article 3 of the Directive no longer being at issue" (European Commission 2007a: p.8).

Actions by Article 29 Working Party

We also recommend that the Article 29 Working Party should seek to clarify some specific points about data protection and privacy within the framework of eGovernment, instead of its adoption of a "general" position about eGovernment as reported in the Article 29 Working Party's (2003) WP 73 Working Document on eGovernment.

Addressing more detailed and up-to-date issues, for example related to PINs and Radio Frequency Identification (RFID), could help to develop specific harmonized 'European common guidelines' or "interpretative communications" in this field; these would contribute to greater clarification for all stakeholders concerned. As such documents are agreed by all representatives of the NSAs (who compose the Article 29 WP), the NSAs are therefore committed to following these guidelines on a series of matters relating to eGovernment at their national level and to provide greater assistance to governments in the implementation of national plans.

Typical examples that could be followed related to the eGovernment sector are the documents already furnished by the EDPS to the European Institutions and bodies (which could be considered as the EU "public administration", even if currently it is not the real legal status of those bodies). The EDPS deals indeed with important issues within the EU bodies that concern all public bodies. Examples of issues already dealt with are: the interoperability of data bases, the role of the Data Protection Officers (DPO) (in ensuring effective compliance with Regulation 45/2001), or the public access to documents and data protection[39]. Furthermore, the EDPS' documents in his role of supervision, produced to the DPOs and the data controllers within such institutions (e.g. opinions, consultations, complaints, etc), are very relevant to reach a common approach on fundamental issues related to all public administrations in general[40].

Actions at the Member States level

Actions by governments and public authorities

First of all, Member States should review or adapt their national laws on data protection in order to be more compliant with Directive 95/46/EC and the recommendations already provided by Article 29 Working Party about such harmonization[41].

Amending national laws in order to give the NSAs an effective independence with regard to governments (e.g. by more financial support in resources) is a basic "precondition" to provide them with the powers to monitor data protection practices within the Member States[42]. As the European Commission (2007a: p. 5) also emphasizes: "one concern is respect for the requirement that data protection supervisory authorities act in complete independence and are endowed with sufficient powers and resources to exercise their tasks. These authorities are key building blocks in the system of protection conceived by the Directive, and any failure to ensure their independence and powers has a wide-ranging negative impact on the enforcement of the data protection legislation."

[39] See "consultation" documents on: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/4.

[40] See "supervision" documents on: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/3.

[41] All Article 29 WP documents can be found on: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm.

[42] In a personal communication, our Project's Expert, Mr. Emilio Aced Félez (Head of the Inspection Unit, Data Protection Agency of Madrid, Spain) emphasized: "Although the adoption by the Working Party of a document means a high degree of commitment by NSAs to follow its guidelines, they cannot overcome national legislation dispositions and, even though the NSAs could fully agree with their contents, sometimes they cannot implement them completely because of the national legal framework". This observation stresses the fact that, before an action can be satisfactorily undertaken by the Working Party together with NSAs, national legislations about data protection should be more harmonized and compliant with the Directive.

As noted before, a “best practice” example in the field of eGovernment is the independent supervisory authority established by Regulation (EC) 45/2001 with regard to European Institutions and bodies: the European Data Protection Supervisor (EDPS). Such Regulation has indeed provided him with important powers, as he is “responsible for monitoring and ensuring the application of the provisions of this Regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data”[43].

However, unlike NSAs powers within certain national legal frameworks, the EDPS is provided with effective enforceable powers[44] to carry out such tasks, such as the right of information, access to all relevant documents, intervention before the European Court of Justice, refer the matter to the EU institutions concerned, etc. His sanctions against the EU bodies concerned could even get to order the “rectification, blocking, erasure or destruction” of the data processing incriminated[45].

Such a solution could also be adopted by Member States in the specific field of eGovernment, in order to give to NSAs specific powers of supervision, consultation and even “coercion” regarding public administrations.

Then, to promote an effective leadership from the “top to the bottom” of the public administrations hierarchy, all national public authorities should provide clear guidance to civil servants about data protection duties and liabilities. The creation of Data Protection Officers (DPOs), who should become compulsory within each relevant public administration, could be a good solution. In fact, Article 18(2) of Directive 95/46/EC opens the door to the appointment of such new “figures”. This should also facilitate the overcoming of the lack of coordination barrier in this field.

Such a solution would lead to improved awareness of data protection matters by the public bodies themselves. It also establishes clear ‘interlocutors’ within public administrations, i.e. specific civil servants (with appropriated skills on data protection issues) to whom citizens and businesses could refer any related issues or concerns they wish to raise regarding the collection and the processing of their personal data by public administrations.

This kind of solution could play a valuable part in overcoming a demand side barrier category - a lack of trust of eGovernment services and, at the same time, it could overcome the workplace and organisational inflexibility barrier on the supply side.

This is already the choice made, for instance, by the data protection laws in France (see French Decree No. 2005-1309 of 20 October 2005, particularly Article 42) and Germany (German Federal Data Protection Act of 15 November 2006, particularly Section 4f and 4g). As it is also the solution provided by Regulation (EC) 45/2001 to the European institutions[46], a “best practice” case that could be transposed into national level is the case of the European Commission. With regard to the size of the institution and the necessity to have relays in its different Directorates-General (DGs), one EU official has been named as ‘top’ DPO of the EC, under the supervision and the control of the EDPS. Under the coordination of the “top” DPO, a ‘pyramidal network’ of internal DPCs has been established (known as ‘Data Protection Coordinators’), one for each DG[47]. The DPO and the DPCs[48] are therefore the ‘guarantors’ of

[43] Article 41, §2 of Regulation 45/2001.

[44] Provided by Article 47 of Regulation 45/2001.

[45] Article 47 (e) of Regulation 45/2001.

[46] Article 24 of Regulation 45/2001 states: “Each Community institution and Community body shall appoint at least one person as data protection officer”. Moreover, this officer (DPO) must cooperate with the EDPS, including providing him/her notifications of processing operations within the related institution that present special risks (e.g. relating to health matters and the evaluation of staff).

[47] For more information about the network of DPOs of the European institutions, see: http://www.edps.europa.eu/EDPSWEB/Jahia/lang/en/pid/36.

[48] The network of the EC DPCs could be found on: http://www.edps.europa.eu/EDPSWEB/Jahia/lang/en/pid/43. One should notice that a specific EC body as OLAF (European Anti-Fraud Office) has its own DPO, due to the “sensitive matters” that it deals with (more information on: http://ec.europa.eu/anti_fraud/index_en.html).

a good and harmonized implementation of Regulation (EC) 45/2001 within this institution by its data controllers. And the EDPS could intervene at any moment to obtain quick information on data processing operations of the EC by those actors.

We recommend that such a network be put in place by all data protection national laws within each public administration authorities, in order to favour a greater knowledge of data protection issues and to create a bigger consensus on data protection principles at all administrative levels. Such an approach should favour a better knowledge by citizens of their rights and risks related to their personal data that could be also beneficial as regard to the private-sector.

Actions by National Supervisory Authorities (NSAs)

As stressed above, one reason for the generally poor effectiveness of national laws about data protection, and therefore of the Data Protection Directive, has been the relative lack of awareness by public entities of their data protection requirements – and by citizens' about their privacy and data protection rights. For instance, Meudal-Leenders (2007) has observed: "European citizens are generally unfamiliar with data protection issues and unaware of their rights in this respect: a 2003 Eurobarometer survey on the protection of privacy in the European Union showed that 70% of European citizens felt they knew little about what was done in their country to protect their privacy".

We therefore suggest to NSAs, and Member States in general, that they should undertake a wide range of actions to promote these rights within civil society. Such awareness-raising policies should have a strong educational element and use a range of traditional and new digital media (e.g. websites of public administrations and bodies). The aim would be to ensure citizens are much better informed about their rights of access to, and rectification of content of, their personal data and other aspects of relevance to the collection and use of such personal data.

A number of such efforts have already been undertaken by the data protection international community (e.g. the European Commission; Central and Eastern Europe Personal Data Protection Commissioners; European Data Protection Supervisor; National Data Protection Authorities (NSAs); and the Council of Europe through the Permanent Representations of the 38 State parties to its 'Convention 108' and the Consultative Committee established by this Convention). These have included achievements within the framework of the 'Data Protection Day'[49], a series of related events held on 28 January 2007, the anniversary of the opening for signature of the Council of Europe's Convention 108 for the Protection of individuals with regard to automatic processing of personal data.

The Data Protection Day aimed to raise awareness among European citizens of data protection issues. It also sought to inform and educate the public at large, and specially targeted groups within it, about their day-to-day rights and good practices in this area in order to enable them to be better able to exercise these rights. In addition, it offered data protection professionals the opportunity to meet the data subjects affected by related legislation. Such initiatives should continue to be supported on a larger scale. Once more, NSAs should be given more financial support by national governments to encourage greater national and local 'working/training days' to discuss common privacy and data protection issues with relevant stakeholders at different levels (national, regional, local, trainings addressed to targeted groups, etc)[50].

[49] Associated awareness-raising events were organized in 29 of the 38 state parties to Convention 108, as well as by the European Commission, the European Data Protection Supervisor and the Council of Europe. Most, but not all, of these events were organized by national data protection authorities (NSAs); in several countries where regional data protection authorities are established, such as Germany and Spain, these regional bodies also played a key role in the Day. For more on this Day see Meudal-Leenders (2007) and http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/Data_Protection_Day_default.asp#TopOfPage

[50] This has already been done at a pan-European level, where examples of agenda topics for such events include: electronic health records; police and criminal aspects; data protection in EU Institutions;

Mr. Emilio Aced Félez, one of the Breaking Barriers project experts, has also stressed that: “there is a clear commitment by NSAs to improve their communication strategies and to foster increasing efficiency in this area, although many of them have limited budgets and resources”. For instance, at the 28th International Data Protection and Privacy Commissioners’ Conference in November 2006[51], a Working Group was set up to explore new ways for sharing the successful experiences of different DPAs (e.g. by highlighting ‘best practice’ cases that should be followed by other stakeholders[52]). A workshop in Paris in April 2007 has also created a network of ‘Communication Officials’ with the aim of sharing its results with all Data Protection Commissioners at the 29th International Conference in September 2007[53]. Such initiatives should be more widely publicized to civil society and within public administration decision-making processes to help maximize their benefits throughout society.

We recommend also that the consultation of NSAs before any governmental decision about data protection issues related to eGovernment matters should be provided by national laws in a compulsory way. This should allow them to provide greater assistance to national governments before the implementation of national plans in a full compliance with data protection laws. Meanwhile, they should increase the publicity of their work already done in the sector of eGovernment[54], and provide public administrations with specific “working papers”/ “opinions” taking up the work done within Art. 29 WP. The European Commission has also invited NSAs to adapt their “domestic practice to the common line” decided by Article 29 Working Party (European Commission 2007a: pp. 9).

Assessing the value of using PINs by public administrations

As discussed in Deliverable 1b, the introduction and use of Personal Identification Numbers (PINs) is an important privacy issue because the power of public administrations can be increased when PINs are used in conjunction with automatic data processing systems. For instance, file interconnections enabled via the use of a unique identifier like a PIN allows administrative bodies to more easily match personal information held in various distinct files in a way that excludes the data subject from the information circuit. The benefits and risks of using PINs need to be carefully assessed as they could threaten certain freedoms when used in some contexts.

An assessment of PINs in terms of ‘power’ raises questions about individual freedoms and control because their use could increase the ‘profiling’ of individuals or ‘tracking’ of citizens. However, the Data Protection Directive Article 8(7) “delegates” to the Member States the power “to determine the conditions under which a national identification number or any other identifier of general application may be processed”. This opens the possibility of differing interpretations of what is required.

For instance, this year, the French Data Protection Authority (CNIL)[55] ruled against the use of a ‘personal identification number’ (NIR)[56] for accessing patients’ medical records. CNIL

media and other issues regarding children and personal data; transborder data flows; and the fight against terrorism (e.g. see Frangou 2007).

[51] For more on the 28th International Data Protection and Privacy Commissioners’ Conference, see http://www.privacyconference2006.co.uk and, in particular, the Closing Communiqué (at: http://ico.crl.uk.com/files/FinalConf.pdf).

[52] For example, the Data Protection Agency of Madrid (of which Mr Aced Félez is Head of the Inspection Unit) has a specific Consultancy Department whose only goal is to instruct and help data controllers to implement data protection policies and to answer their doubts and problems. Even though there is no legal regulation in Spain regarding DPOs, Mr. Aced Félez has helped the Madrid DPA to set up a network of data protection coordinators in every General Directorate of the government of the Region of Madrid and in its city councils.

[53] For more information on this conference, see: http://www.privacyconference2007.gc.ca/Terra_Incognita_home_FR.html

[54] As it is the case for the French example of the CNIL (relevant documents and information on: http://www.cnil.fr/index.php?1007).

[55] See the CNIL’s website on: http://www.cnil.fr/

[56] NIR is the Numéro d’Inscription au Répertoire National d’Identification des Personnes Physiques, the ‘National Index for the identification of individuals’ (see CNIL 2004).

believes the use of the NIR as a means of accessing patients' medical records is "clearly inappropriate, as health data is particularly sensitive and should be given greater protection than can be provided by such a system". CNIL instead proposed the use of a specific identification number for accessing medical records, based on the patient's NIR – but anonymized. This was also the position adopted by the Health Professions Act passed on 1 February 2007. Nevertheless, the French government ruled in favor of the use of the NIR for this purpose (Le Monde 2007), and has not taken into account this alternative view.

Recommended solutions

Against this background, it would be desirable to establish a common understanding on the benefits of using identifiers like PINs, as well as the risks raised by them in terms of data protection issues. A key aim would be to lead a move towards a more harmonized European legal framework on this question. Such movement could, at the moment, only be realized either by the Article 29 Working Party at a pan-European level, or/and by NSAs at the national levels (if their national legislation would allow them). This could begin minimally by compiling all Working Papers and Opinions of the Article 29 Working Party about related issues into one larger communication regarding eGovernment, such as a 'European Guide'. This would provide clear, pro-active guidance to all stakeholders on how to implement a good eGovernment service taking into account the risks and values of the use of PINs. Such a "Guide" could then be used by NSAs at national level, to help them to provide clear guidance to public administrations on specific topics related to the use of PINs.

However, it is still a very sensitive topic for Member States because there are many different sensibilities within Europe regarding this matter, arising from the different cultures and histories within Member States. As Mr. Aced Félez has commented[57]: "in my view, the moment has not come yet for Member States to give up their sovereign powers in this field".

Nevertheless, the development of a "best practices" cases framework in the field of eGovernment could be of great help for both actors mentioned above, in order to provide experts' assessments of the different kinds of PINs that exist, and the advantages and risks that they could entail[58].

Facilitating the use of PETs

The application of Privacy Enhancing Technologies (PETs) could help to enhance the level of privacy and data protection within public administrations. Ensuring PETs are applied in the most effective manner where they offer relevant safeguards is therefore another key privacy and data protection issue.

The value of PETs to achieving privacy and data protection goals in the EU was recently underlined in a European Commission (2007b) Communication that sets out clear actions for supporting the development of PETs and their use by data controllers and consumers. The Commission stresses this could be of assistance in pursuing the aim of the existing legal framework that minimizes the processing of personal data and encourages using anonymous or pseudonymous data wherever that is possible. It sees PETs as helping to ensure "breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions, but technically more difficult".

Recommended solutions

The European Commission (2007b) Communication adopts the definition of a PET as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system". Furthermore, such tools should be stand-

[57] Personal comment based on his personal experience with moves to an electronic version of the Spanish National Identity Card (DNI), about which much trust has been built within the Spanish context.

[58] Such moves could complement or be part of ePractice.eu

alone aids requiring positive action by consumers (who must purchase and install them on their PCs) or be built into the "very architecture of information systems". The Commission argues that the use of PETs can help to design information and communication systems and services "in a way that minimizes the collection and use of personal data and facilitates compliance with data protection rules".

Such a solution could contribute to overcoming the demand side barrier – a lack of trust of eGovernment services, as users should no longer feel the compulsory collection of their data by public administrations as a dangerous tool of the "Big Brother's State" against them. When protection and security of personal data are real and ensured, such fear would be reduced[59].

Furthermore, the use of PETs by public administrations should contribute to the diffusion at a larger scale of safe privacy's practices within Member States, and increase awareness on those matters by all actors, that could also be used further by the private-sector operators.

Examples of PETs mentioned in this Communication include:

- automatic anonymization of data after a certain lapse of time: supports the principle of processed data being kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data were originally collected;
- encryption tools: prevent 'hacking' and other forms of unwarranted accessing of information when it is transmitted over the Internet, and support the data controller's obligation to take appropriate measures to protect personal data against unlawful processing;
- cookie-cutters: block 'cookies' placed on users' PCs by websites and other sources to make the user's system perform certain instructions without the user being aware of these actions, thereby enhancing compliance with the principle that data must be processed fairly and lawfully, with the data subject being informed about the processing involved; and
- the Platform for Privacy Preferences (P3P): allows Internet users to analyze the privacy policies of websites and compare them with the users' preferences regarding the information they wish to release, helping to ensure that the consent of data subjects to the processing of their data is an informed one.

Furthermore, in order to ensure the respect for appropriate standards in the protection of personal data through the use of PETs, standardization and coordination of national technical rules on security measures for data processing are also envisaged by the Commission. For instance, it intends to conduct actions to raise consumers' awareness and to investigate the feasibility of an EU-wide system of "privacy seals"[60], which would allow consumers to easily recognize a certain PET product as ensuring or enhancing respect for the appropriate data protection rules.

[59] It is interesting to note that in the private sector, in some countries (as it was stressed by an Italian participant in a recent project's workshop), and especially with the new phenomenon of online social networks, users often do not hesitate to widely furnish their personal data to some websites, which are even not fully compliant with the European data protection legislation (see ENISA 2007). However, they do not trust web services provided by public administrations and hesitate to give personal information via the Internet to them. This is not the case everywhere, as in Spain or in Greece, for instance, there is more confidence in the public sector than in the private-sector, as it has been reported by other participants (see our Sixth workshop report: "Solutions for eGovernment", 16/11/2007, on pp.7-9, http://www.egovbarriers.org/downloads/Oct21Workshop/200710_workshop_6_report.pdf).

[60] See, for instance, the EuroPriSe European Privacy Seal project (under the eTen Programme), a consortium of eight European organizations and enterprises led by the Independent Centre for Privacy Protection Schleswig-Holstein (ICPP/ULD) that have combined forces to produce a European Privacy Seal (http://www.epractice.eu/document/3682 and http://ec.europa.eu/information_society/activities/eten/library/news_release/doc/europrise.pdf).

Better balancing interoperability v. data protection requirements

As discussed in deliverable 1b, interoperability of personal data between public bodies should not be sought at all costs. Certain key legal requirements relating to data protection must not be abandoned, even if they cause interoperability problems (e.g. the respect of the 'purpose principle' - that personal data must be collected only for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes[61] - is even more relevant in the day-to-day practice of public administrations). This is particularly important for activities that might breach the protection of privacy as a fundamental right.

Interoperability barriers arise in pursuing improved administration effectiveness and simplification through eGovernment initiatives. In these circumstances, certain information must also be protected and be limited only to the public administration allowed to process it, in accordance with the purpose principle and the proportionality requirement, there is always the necessity to continually balance the different interests at stake. In a democratic society, one reason for law in this field is to protect citizens against powerful institutions and to limit actions that could endanger their safety and the protection of their personal interests (e.g. personal data, privacy, freedom, autonomy). In this respect, Directive 95/46/EC seems to strike the right balance between conflicting values affecting interoperability and data protection, including guidelines on what has to be done in processing personal data to ensure the effective protection of personal information within the EU.

National and other government bodies at all levels hold much compulsory information. This could become dangerous for the autonomy or even safety of individuals if an authoritarian, non-democratic government comes to power or if abuses arise in addressing public security concerns, such as in the 'fight against terrorism'[62]. eGovernment is therefore a sector where processes involved in personal data transfers between governments or public bodies should be highly transparent and controlled by an independent body.

Recommended solutions

It is important to emphasize that citizens and businesses base their relationships with public administrations mainly on trust and confidence in government's protection of their interests. However, the lack of trust is a relevant remaining barrier to be overcome in this field (see also discussions in deliverable 1b on Authentication and Identification and on Public Administration Transparency).

As a result, we recommend a wide promotion of individuals' privacy rights at a European level, which would then be implemented at national and local levels, by all actors mentioned above in the section on Overcoming Disparities in Implementations of the Data Protection Directive. This should be combined with a greater transparency of the public bodies' processes, controls and guarantees. Together, these initiatives should contribute to increased trust and confidence in eGovernment in general, as well as in relation to data protection issues in particular.

We also endorse the recommendations of a recent Modinis study to the European Commission on matters relating to interoperability at local, national and pan-European levels (see Tambouris et al. 2007: 64–6). This advice includes:

- At the EU level: encourage harmonization in administrative practices among Member States.
- For policy making and management: promote a common terminology in important specific 'vertical' application areas (e.g. electronic Identity Management).

[61] See Article 6(1b) of Directive 95/46/EC, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf

[62] For example, the concerns expressed by the Secretary General of the Data Protection Authority of Italy, Giovanni Buttarelli (2007).

- In the technical area: create a European eGovernment interoperability (IOP) infrastructure (e.g. a Web portal for classifying local authority services; promoting re-use; and documenting best practices and relevant experiences).

Conclusions

Regarding the first barrier (disparities in implementation of Directive 95/46/EC), following the provisions of Article 6 of the “Treaty of Lisbon” (the new Reform Treaty), approved during the Informal European Council in Lisbon on the 18-19 October 2007[63], the Charter of Fundamental Rights of the European Union of 7 December 2000 (that recognizes the right to privacy and data protection in its Articles 7 and 8) will have from now on the same legal value as the Treaties[64] (except in Poland and the United Kingdom[65]). Furthermore, the right to the protection of personal data in itself is recognized by the new Article 16B of the Treaty, which states that:

> *“1. Everyone has the right to the protection of personal data concerning them.*
>
> *2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*
>
> *The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 25a of the Treaty on European Union."*

Nevertheless, such recognition should not change radically the state-of-art in this field, as it is rather the resistance to change and the Member States cultural and historical disparities that postpone a full harmonization of Directive 95/46/EC[66] than the “non-existence” of legal binding texts.

Furthermore, as the EDPS (2007a) has stressed, this new Treaty does not seem to take into account all the legislative progress made within the data protection field. For instance, it does not take into account the existence and the role already in force of the EDPS (2007a: p. 1

[63] This new Treaty will be signed by the Member States on 13 December 2007 by the Member States. The signature of the Treaty will be followed by the ratification process in all 27 countries. It is hoped that the new Treaty will come into force before the next European Parliament elections in June 2009 (see information on: http://europa.eu/reform_treaty/index_en.htm).

[64] The new version of Article 6 states indeed that “1. The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties. The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties. The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.”

[65] See relevant Protocol on the Treaty. Moreover, as the former French President Valéry Giscard d’Estaing has emphasized in a press article, the concessions made for the British (respect to the older version of the Reform Treaty, previous called “Constitutional Treaty”) are relatively important in this field, as “the Charter of Fundamental Rights – an improved and updated version of the Charter of Human Rights – has been withdrawn from the draft treaty and made into a separate text, to which Britain will not be bound” (see *The Independent*, 2007). This is clearly a step backwards in relation to the older version of the Treaty in the field of data protection, where all Member States are not “playing in the same ground”. This will not contribute to such a good harmonisation of the data protection legislation and practices within the European Union, despite the Commission’s and EDPS’ opinions (see Commission 2007a and EDPS 2007a and 2007b).

[66] Recently, the EDPS (2007b: pt 3 and 4) has also emphasized that “in the short term Directive 95/46/EC should not be amended”, as “considerable improvements in the implementation are still possible”, nevertheless “in the longer term, changes of the Directive seem unavoidable, while keeping its core principles” and “a clear date for a review to prepare proposals leading to such changes should already be set now” in order to “give a clear incentive to start the thinking about future changes already now.

about “Article 24”) [67]. How to make improvements in this field if other EU political institutions (the new Treaty has been adopted by the Representatives of the Governments of the Member States) do not take into account the work done since 1995, at least?

As regards the lack of awareness of data protection rights, it is particularly important to stress that providing specific training to young generations about data protection and privacy issues, at an early stage (e.g. by integrating such training in the school programme, as a citizen’s new “civil right”), should also become a political priority of Member States. It is possible, that the progress of Web 2.0., for instance, will lead to more invasion of the private sphere without real awareness of it (see ENISA 2007), and all stakeholders in the field of data protection should be vigilant with regard to this issue[68].

As we have emphasized before, further work should be undertaken at many levels (European, national, local) as regard personal data and the protection of the data subjects’ rights in the field of eGovernment: clear assessments of PINs and interoperability of systems are only some examples of that. For instance, the Commission should pursue its analysis regarding PETs, as other questions may arise, such as: Who will be in charge of the integrity of such systems? Should NSAs become responsible for the long term monitoring of those practices within public bodies ? Should another “independent authority” be created in order to certify possible “privacy seals”? Who will be responsible in case of failure of the systems (the data controllers, the processors, the technical subcontractors)? In this context, the financial inhibitors that may arise is only the “tip of the iceberg” that should be considered in the future.

It is important that all EU political institutions and specifically the Member States governments take effectively into account the work already done by European experts of data protection, such as the EDPS (as regard eGovernment issues) and the Article 29 Working Party (in general), in order to guarantee effectively the citizens’ fundamental rights already promoted at European level. Overcoming legal barriers is irrelevant if there are not effective political actions behind these changes.

References

Article 29 Data Protection Working Party (2003), Working Document on eGovernment, Adopted on 8 May, 10593/02/EN, WP 73, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/e-government_en.pdf

Buttarelli G. (2007), General Secretary of the Data Protection Authority of Italy, eGovernment, eDemocracy and Data Protection: The Italian Experience, Data Protection Review, No. 2, February, http://www.dataprotectionreview.eu

CNIL (2004), Commission Nationale de l’Informatique et des Libertés, La Position de la CNIL sur le Programme ADELE (Administration Electronique), 26 February, http://www.cnil.fr/fileadmin/documents/approfondir/dossier/e-administration/ADELE2004.pdf

ENISA (European Network and Information Security Agency) (2007), Security Issues and Recommendations for Online Social Networks, Position Paper N°1, October, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

European Commission (2007a), Communication from the Commission to the European Parliament and the Council on the follow-up of the Work programme for a better implementation of the Data Protection Directive, COM(2007) 87 final, 7/3/2007, Brussels:

[67] The EDPS (2007a) has stressed the importance to take into account the role of the EU institutions in data protection issues, as he has suggested: “Article 24 [a specific provision on data protection for the area of the Foreign Common and Security Policy]only refers to activities of the Member States, not of activities of the Union. It should also apply to activities of the Union, for instance if the Council at a certain stage will process a terrorist list.” If we read the new text adopted the redaction of Article 25a (ex-24) has not taken into account the EDPS’ suggestions.

[68] Once more, the EDPS (2007b) highlighted also that: “The information society is evolving and has more and more characteristics of a surveillance society. This implies an increasing need for effective protection of personal data to deal with these new realities in a fully satisfactory way”.

European Commission, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf

European Commission (2007b), Communication from the Commission to the European Parliament and the Council on promoting data protection by Privacy Enhancing Technologies (PETs), COM(2007) 228 final, 2/5/2007, Brussels: European Commission, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0228:EN:NOT

European Data Protection Supervisor (EDPS) (2007a), Data protection under the Reform treaty in the intergovernmental conference (IGC), Letter to the IGC presidency and Annex, 23 July, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2007/07-07-23_Letter_IGC_EN.pdf and http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2007/07-07-23_Annex_IGC_EN.pdf

European Data Protection Supervisor (EDPS) (2007b), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, Official Journal of the European Union C255, 27 October, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.pdf

Frangou, G. (2007), Data Protection Commissioner of Cyprus, Review of the Spring Conference of the European Data Protection Authorities (Larnaka, Cyprus, 10-11 May 2007), Data Protection Review, No. 3, June, http://www.dataprotectionreview.eu

Le Monde (2007), 'The French CNIL Recommends the Creation of a Specific Number, Based on the Personal Identification Number, to Access Medical Records', Le Monde, 25 June, Data Protection Review, No. 3, June, http://www.dataprotectionreview.eu

Meudal-Leenders, S. (2007), Head of the Data Protection Unit, Directorate General of Legal Affairs, Council of Europe, Review of the First Data Protection Day, Data Protection Review, No. 2, February, http://www.dataprotectionreview.eu

Tambouris, E., Tarabanis, K., Peristeras, V. and Liotas, N. (2007), Study on Interoperability at Local and Regional Level (2007), Interoperability Study Final Version – Version 2.0, MODINIS Lot 2, 20 April, http://ec.europa.eu/information_society/activities/egovernment_research/doc/interop_study.pdf

The Independent (2007), 'Valéry Giscard d'Estaing: The EU Treaty is the same as the Constitution', The Independent, 30 October, http://comment.independent.co.uk/commentators/article3109902.ece

EU-level, national and other relevant legislation and regulations

Note: All information on applicable law on data protection in the EU is available at: *http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm*

Charter of Fundamental Rights of the European Union, Official Journal of the European Communities C 364, 18 December 2000, http://www.europarl.europa.eu/charter/pdf/text_en.pdf

'Convention 108', the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS No. 108, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281, 23/11/1995, pp. 31-50, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (an updated status of this Directive's implementation is available at: http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm).

French Decree No. 2005-1309 of 20 October 2005, J. O. No. 247 of 22/10/005, p.16769 Text No. 31, http://www.cnil.fr/fileadmin/documents/uk/Decree_20_October_2005_English_version.pdf

German Federal Data Protection Act (Bundesdatenschutzgesetz) as of 15 November 2006, http://www.bfdi.bund.de/cln_029/nn_535764/EN/DataProtectionActs/DataProtectionActs__node.html__nnn=true

Regulation (EC) 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, http://ec.europa.eu/justice_home/fsj/privacy/docs/application/286_en.pdf

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

Public Administration Transparency

Professor Cécile de Terwangne and Dr Cristina Dos Santos

Centre de Recherches Informatique et Droit (CRID), University of Namur, Belgium

Introduction

Freedom of Information (FOI) Acts are the prime legal vehicle for promoting public administration transparency through eGovernment. An important indication of the barriers to such transparency is therefore highlighted by the exceptions to transparency contained in different FOI Acts, which can vary according to the different legal, historical and political traditions in Member States.

A key problem with transparency in relation to eGovernment is the general lack of public awareness of the availability of the vast range of information held by public bodies, as well as difficulties in locating the information needed for a particular purpose. Improvements in these areas would contribute to a better understanding in two key areas: the internal functioning of the public administration as an entity; and the actions undertaken by civil servants and officials in decision-making processes, which could also be related to the transparency of the political decision-making process in the fields of eDemocracy and eParticipation.

Inadequate access to appropriate technological tools or the lack of user skills in electronic media are further constraints on the achievement of the kind of transparency envisaged by many who support FOI and related legislation. In addition, traditional FOI Acts are mainly focused on transparency provisions that are 'passive' (information requested by a citizen) as opposed to 'active' (information spontaneously made available by government). Although, there is a trend towards promoting the latter, more active approach.

'Active transparency' means public authorities accept responsibility for making information publicly available. There are serious divergences between EU Member States on this point. For instance, some newer Member States have recently adopted FOI legislation containing detailed provisions promoting active transparency, which requires the information to be made available through an electronic public network such as the Internet. On the other hand, most of the more 'ancient' FOI laws are deficient as regards compulsory publication of public sector information (see examples provided in Deliverable 1b).

One of the barrier categories identified in Deliverable 1b of this project most relevant to this area is that of digital divides and choices. This is represented by the way knowledge and skills are distributed among users and potential users who might wish to gain access to electronic networks, for example in the extent to which easy-to-understand 'meta-data' overview guides are provided to help find what information is available. Information requests can be discouraged in those countries where the fees charged for such access are perceived as being too high. Language can also be an important barrier (e.g. when a minority language is not well supported online), even when transparency is legally guaranteed in a Member State.

Further specific action in addressing issues relating to digital divides and inclusion are foreseen in the European Commission's (2005a) Communication on eAccessibility and its Agenda for eInclusion planned for 2008, as part of the i2010 action plan (European Commission 2006a) (which was reinforced by the Lisbon Ministerial Declaration of the 19th of September 2007 where Inclusive eGovernment was identified as a key priority policy action). However, there is a general lack of coordination at the EU level with regard to access to public sector information, except for some sectors covered by their own specific Directives, such as for information on the environment (e.g. Directive 2003/4/EC) or public procurements (e.g. Directives 2004/17/EC and 2004/18/EC).

Structural barriers add to coordination difficulties (e.g. the federal structures of some States accentuate the disparity of access policies). There are also significant differences between Member States or regional levels (e.g. in provisions for active transparency and restrictions on access).

Nevertheless, transparency is now generally seen to be a fundamental condition for public trust in government activities, including eGovernment services. Therefore, in the many Member States where there is a lack of tradition for openness, a change in public administration culture is needed to help build trust in eGovernment. This could be supported by more emphasis on active transparency.

As EU Member States have traditionally had prime responsibility for transparency issues, there has been a general lack of FOI general legislation at the European level.[69] The exceptions made for information in areas like the environment and public procurement have been justified by the principle of subsidiarity. This principle means the Union takes action only in the areas that fall within its exclusive competence, and not where action is more effectively taken at a national, regional or local level. It is closely bound up with the principles of proportionality and necessity, which require any action by the Union to avoid going beyond what is necessary to achieve the Treaty's objectives.

Recommended solutions: Actions by the European Commission

The EC is not empowered to issue a proposal for a directive dealing with general access to PSI. Nevertheless the EC could be interested to follow less formal ways of harmonizing things. Adopting a common vision across the EU about transparency could be valuable. The aim should be to develop a kind of 'European model' of an FOI Act, more precisely as concerns electronic FOI and active transparency.

To launch a detailed study on the Member States 'FOI culture'

The EC could launch a detailed study at the European level on the state-of-the-art of 'FOI culture' of the different Member States. This study would go beyond the mere gathering of all relevant acts - which has already been done by the EC. It would lead to getting information on actual realizations, on concrete operations and applications, especially with regard to the active dissemination of PSI.

A study of FOI cultures in the EU could contribute to realizing a degree of further harmonization between national laws of Member States, at least regarding 'passive transparency' measures. This should also take into account other problems identified in Deliverable 1b, such as national disparities between costs, access to electronic formats and the lack of meta-data guides. The study could form a basis for proposing concrete measures to be undertaken by the European Commission together with Member States.

To reinforce and reorient Public Administration Transparency

The path to achieving more effective transparency was indicated on 9 November 2005 when the European Commission launched its European Transparency Initiative within the European institutions. As stated in a Green Paper on the Initiative (European Commission 2006b), it aims "to ensure that the Union is open to public scrutiny and accountable for its work (…) [as] the European public is entitled to expect efficient, accountable and service-minded public institutions and that the power and resources entrusted to political and public bodies are handled with care and never abused for personal gain". It intends to build on a series of transparency-related measures already put in place by the Commission, in particular those taken as part of the overall reforms that have been implemented since 1999, including the White Paper on European Governance (European Commission 2001).

[69] The European Charter of fundamental rights provides (art. 42) a right to access to public sector documents but only for what concerns European Parliament, Council and Commission. Art. 255 EC Treaty opens the same right and gives more detailed. The ModifyingTreaty (art 255 became art. 15 in the October 2007 version) slightly modifies the scope of the access right as it opens it towards all European institutions, organs and agencies. There is of course no consecration of a general right of access through the 27 Member States.

There have been some major achievements in this field, such as: ‘access to documents’ legislation, as in Regulation (EC) No 1049/200170; the launch of databases providing information about consultative bodies and expert groups advising the Commission; and wide stakeholder consultation and in-depth impact assessments prior to legislative proposals. In addition, the Commission’s (2006b) Code of Good Administrative Behaviour has sought to become its “benchmark for quality service in its relations with the public”. The professional ethics of Commission staff are regulated in its Staff Regulations and implementing rules. At the political level, the EC Treaty includes clear provisions on the ethical standards to be observed by Members of the Commission. These have been put into operation through the Code of Conduct for Commissioners.

A follow-up to the European Transparency Initiative has set out the next steps the Commission will take to identify and stimulate a debate on areas for improvement (European Commission 2007). This includes a review[71] of Regulation 1049/2001 as part of the Commission’s policy of creating more openness based on “a partnership of (public) consultation and participation”. The review seeks to ensure proper account is taken of the concerns of citizens and all other interested parties, as essential contributions to implementing the Commission’s ‘better lawmaking’ policy (e.g. see the European website ‘Your Voice in Europe’[72], which gathers information on all consultations carried out by European Commission Directorate-Generals).

Two of the main objectives of the European Commission’s (2006a) i2010 Action Plan already have a focus on transparency that were reinforced by the Lisbon Ministerial Declaration of the 19th of September 2007. One is: “Making efficiency and effectiveness a reality – significantly contributing, by 2010, to high user satisfaction, transparency and accountability, a lighter administrative burden and efficiency gains”. The other, which refers to the Commission’s European Transparency Initiative, is the eParticipation aim: “Strengthening participation and democratic decision-making in Europe”.

As the European Commission (2006a) notes: “Countries that score highy on public-sector openness and efficiency and eGovernment readiness are also top on the economic performance and competitiveness scoreboards”[73].

There would also be much value in undertaking a similar initiative at a pan-European level regarding the “transparency of the public sector” more generally. However, this is a very sensitive legal field where traditional concerns about national sovereignty and competences are still strong. We therefore recommend that the European Commission’s priority should be to seek to create a consensus regarding transparency within Member States.

To organize workshops with Member States to share views, information and experience

An important first step towards this would be to establish more opportunities to share information on transparency experiments among Member States. Organizing workshops at the pan-European level to allow such sharing of views and information would help Member

[70] This Regulation “provides the framework for access to the unpublished documents of the EU institutions and bodies through register of documents or following individual requests”. The Commission has also created a register of documents (as required by the Regulation) plus a special register of documents related to work of the ‘comitology’ committees” (European Commission 2006b). ‘Comitology’ is a procedure established by Article 202 of the EC Treaty which allows the creation of committees that act as forums for discussion. See also Section 8.3 and http://europa.eu/scadplus/glossary/comitology_en.htm

[71] The Green Paper on the Initiative (European Commission 2006b) is the starting point for this consultation, which allows “any interested person” to have a say on related issues. On the basis of this consultation, the Commission will submit proposals for amending the regulation by October 2007 (for more information, see: http://ec.europa.eu/transparency/revision/index_en.htm).

[72] See http://ec.europa.eu/yourvoice/consultations/index_en.htm and the detailed study on Your Voice in Europe in our project’s Deliverable 2 Case Study Report (Section 2.4).

[73] For instance, European Commission (2006a) includes World Economic Forum Global Competitiveness Reports relating to the European Commission Innovation Trendcharts and Scoreboards in the UN Global eGovernment Readiness Reports for 2003, 2004 and 2005.

States to learn from each others' experience, including those who have already launched active transparency initiatives. This would be especially valuable for States which have not yet reviewed their ancient paper-based FOI Act to adapt it to the electronic reality.

This sharing of information could inspire Member States notably to determine active transparency policies and could lead to the development of more common conceptions of how to address related issues.

To issue guidelines towards a common view on FOI

The first two steps should allow the Commission to issue initial guidelines towards a common view on FOI.

These guidelines would notably aim at

- lessening the disparities in costs charged for accessing to PSI between Member States
- addressing the access to electronic formats
- addressing the problem of lack of complete and uniform (in all Member States and within European institutions) meta-data guides to identify available public documents and lack of uniform and successful search engines to locate the desired documents.[74] There is crucial need for pan-European standards to elaborate meta-data guides. The meta-data guides should at least indicate: the identification of the documents or categories of documents, their date, their availability (either published or on demand), their location (if published), the body responsible to allow access (if access on demand).
- addressing the active dissemination of PSI: clarify which categories of PSI are to be actively electronically published; deadlines for publication; form of dissemination (centralized or not)

To propose constraining transparency rules in areas of implicit competences

Whereas the EC has no competence to issue a legally binding instrument dealing with global availability of PSI, it could focus on certain types of information the public availability of which could be seen as linked to an area of EC competence. Issuing a legally binding rule that requires rendering this information publicly available would then be considered as the exercise of an implicit competence.

One could suggest to elaborate a directive requiring Member States to make publicly available all the information necessary to exercise the freedoms and rights guaranteed by the EU Treaty (freedom of establishment, of movement,…).

A small part of this work has already been done in the article 7 of Directive 2006/123/EC on services in the internal market[75]. This article entitled 'Right to information' states that:

> *1. Member States shall ensure that the following information is easily accessible to providers and recipients through the points of single contact:*
>
> *(a) requirements applicable to providers established in their territory, in particular those requirements concerning the procedures and formalities to be completed in order to access and to exercise service activities;*
>
> *(b) the contact details of the competent authorities enabling the latter to be contacted directly, including the details of those authorities responsible for*

[74] The EC has already pointed the necessity of ensuring the 'searchability' and comparability of data for what concerns data on shared management (publication of beneficiaries of EU funds): European Commission (2007) p. 8

[75] Directive 2006/123/EC of 12 December 2006 on services in the internal market, OJEU, 27.12.2006, L 376/36

> *matters concerning the exercise of service activities;*
>
> *(c) the means of, and conditions for, accessing public registers and databases on providers and services;*
>
> *(d) the means of redress which are generally available in the event of dispute between the competent authorities and the provider or the recipient, or between a provider and a recipient or between providers;*
>
> *(e) the contact details of the associations or organisations, other than the competent authorities, from which providers or recipients may obtain practical assistance.*
>
> *2. Member States shall ensure that it is possible for providers and recipients to receive, at their request, assistance from the competent authorities, consisting in information on the way in which the requirements referred to in point (a) of paragraph 1 are generally interpreted and applied. Where appropriate, such advice shall include a simple step-by-step guide. The information shall be provided in plain and intelligible language.*
>
> *3. Member States shall ensure that the information and assistance referred to in paragraphs 1 and 2 are provided in a clear and unambiguous manner, that they are easily accessible at a distance and by electronic means and that they are kept up to date.*
>
> *4. Member States shall ensure that the points of single contact and the competent authorities respond as quickly as possible to any request for information or assistance as referred to in paragraphs 1 and 2 and, in cases where the request is faulty or unfounded, inform the applicant accordingly without delay.*
>
> *5. Member States and the Commission shall take accompanying measures in order to encourage points of single contact to make the information provided for in this Article available in other Community languages. This does not interfere with Member States' legislation on the use of languages.*
>
> *6. The obligation for competent authorities to assist providers and recipients does not require those authorities to provide legal advice in individual cases but concerns only general information on the way in which requirements are usually interpreted or applied.*

A thorough reflection on what information is necessary to exercise all the rights and freedoms warranted in the EC Treaty could lead to enlarging the ‘right to information’ mentioned in the 2006/123 Directive to a comprehensive right implying a correlative duty for the public sector to make various kinds of information available either on demand or by publishing it.[76]

Recommended solutions: Actions by the Member States and EU institutions

- *To ensure public awareness of their FOI rights*: Member States should try to raise public awareness of their FOI rights through public actions promoting these rights
- *To ensure public sector knowledge of the fundamental transparency rules and the confidentiality exceptions:* Initiatives should be taken to support the competences and

[76] Such a right to information already exists for environmental information (see Directive 2003/4/EC of 28 January 2003 on public access to environmental information) We also find in the Follow-up to the Green Paper ‘European Transparency Initiative’ (European Commission 2007) another example of EC initiative taken to have MS publish information about the beneficiaries of EU funds: ‘The Commission fully acknowledges the need for searchable and comparable data and, as a further step, will in autumn 2007 propose a common standard for the publication of data on shared management, so as to enable interested parties to carry out consistent analyses across EU (…)’. Other rights to information exist but we have to consider here, in the eGovernment context only those rights concerning public sector information.

cultural and organizational enhancements needed to ensure the efficiency and effectiveness of FOI laws, and to contribute to the development of an FOI culture. This could include organizing working or training days by relevant themes (e.g. mobility or the environment), addressed to civil servants at national and local levels.

- *To pay attention to the language accessibility of published documents*: Member States should consider the question of language accessibility of the documents publicly available. The use of semantic tools could help to deal with this question even if they cannot completely solve it.
- To review national FOI Acts where necessary to adapt them to the electronic reality
- *To review national FOI Acts where necessary to consider the current trend of developing active transparency:* (i.e. obligation for public bodies to spontaneously render series of information publicly available)

References

Publications

European Commission (2001), European Governance – A White Paper, COM(2001) 428 final, Brussels: European Commission, http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0428en01.pdf

European Commission (2005a), Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee and the Committee of the Regions. eAccessibility, SEC(2005)1095, COM(2005)425 final, Brussels: European Commission, http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0425en01.pdf

European Commission (2005b), E-Commission: Enabling Efficiency and Transparency, IP/05/1474, 25/11/2005, Brussels: European Commission, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/1474&format=HTML&aged=0&language=EN&guiLanguage=en

European Commission (2006a), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, i2010 eGovernment Action Plan – Accelerating eGovernment in Europe for the Benefit of All, SEC(2006) 511, COM/2006/0173 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0173:EN:NOT

European Commission (2006b), Green Paper on European Transparency Initiative (ETUI), COM (2006) 194 final, 3/5/2006, Brussels: European Commission, http://ec.europa.eu/transparency/eti/docs/gp_en.pdf

European Commission (2006c), e-Commission 2006-2010: Enabling Efficiency and Transparency, Brussels: European Commission, http://observatorio.red.es/documentacion/actualidad/boletines/e_Commission06_10.pdf

European Commission (2007), Communication from the Commission, Follow-up to the Green Paper European Transparency Initiative, SEC(2007) 360, COM(2007) 127 final, 21/3/2007, http://ec.europa.eu/civil_society/docs/com_2007_127_final_en.pdf

EU-level, national and other relevant legislation and regulations

Directive 2003/4/EC of 28 January 2003 on public access to environmental information, Official Journal of the European Union, L 041, 14/02/2003, pp. 26-32, http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_041/l_04120030214en00260032.pdf

Directive 2004/17/EC of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors, Official Journal of the European Union, L 134, 30/4/2001, pp. 1-113, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

Directive 2004/18/EC of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, Official Journal of the European Union, L 134, 30/4/2001, pp. 114-240, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en01140240.pdf

Regulation (EC) 1049/2001, of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, Official Journal of the European Communities L 8/1, 12/1/2001, http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_145/l_14520010531en00430048.pdf

Relationships between Public Administrations, Citizens and other ICT Actors

Dr Julián Valero Torrijos

Department of Administrative Law, University of Murcia, Spain

Introduction

One of the main conditions for the success of any initiative related to eGovernment is the guarantee of effective communication between all the parties concerned. From the perspective of citizens, it is essential to be able to gain appropriate access to a range of electronic public services. Otherwise, citizens are likely to find that the only ePublic Services available to them are those they do not consider to be of most value to their own lives.

This demand has created growing pressure for policies and actions that go more deeply into a citizen-focused approach to eGovernment developments. For instance, the Capgemini (2004) eEurope eGovernment Report warns that services must be developed to deliver real value to citizens in return for their taxes invested in the service, rather than to offer primarily the services that mostly interest governments. The Capgemini (2005) report adds that great improvements have been made in electronic services targeted at companies than those seeking to meet citizens' needs. Making a user-centred philosophy a more widespread eGovernment reality requires legal and institutional changes, such as the European Commission's (2005) CoBrA Recommendations to the eEurope Advisory Group.

Nevertheless, in some circumstances it may be impractical (e.g. too costly) to assure there is appropriate access, for instance by having multiple online and offline public service channels suited to different user groups. In such cases, it may be necessary to impose the use of a particular ePublic Service as the only means of contacting public administrations. An alternative could be to facilitate electronic contact with public authorities through intermediaries, such as telephone call centres or a community advice centre with public online access points. Such an alternative may be required, for instance, if the imposition of an online service may be a legal and/or constitutional obstacle.

Among many other issues in this area discussed in the section on Relationships in Deliverable 1b of our project, special attention must be paid to the relationships between public administrations and ICT companies. However, the perspective of citizens should be considered as a priority for providing legal solutions, as required by the European Commission's (2006) eGovernment Action Plan. This section suggests solutions to two of the obstacles identified in Deliverable 1b of particular importance in this area: the provision of a general right for citizens to use electronic means to access eGovernment services, especially those pan-European public services with a "high impact"[77]; and support for a multi-channel approach, including the use of intermediaries to deliver and help access to public services.

Establishing a general eRight for citizens to use electronic means to access public services

The need for an 'eRight' to use ICTs to contact and engage with government

One of the main barriers to eGovernment regarding the relationships between citizens and public administrations is the lack of a general 'eRight' for citizens to use electronic means to contact and engage with government to exercise their rights and fulfil their obligations. Such a legally-assured eRight to use online services in all relations with a public administration could help to overcome poor motivation and confidence towards eGovernment caused by the availability of only a narrow range of predetermined services. A wider understanding of the nature of eGovernment services available to citizens would also be promoted by having a

[77] High impact is the term used in the European Commission (2006) i2010 eGovernment Action Plan.

legal guarantee that citizens must be able to contact relevant public administrations by electronic means to request information and obtain an effective and quick answer.

The strong pressures to use limited public financial resources in the most efficient and effective way mean the intensity of technological eGovernment modernization may vary according to factors other than legal dimensions, including political considerations – particularly in the case of local administrations. This can lead to eGovernment being seen as a lower priority than other investments (e.g. building a new hospital). Without a legal obligation regarding a citizen's eRight to access government services, public administrations are therefore likely to use their wide discretionary power to prioritize according to varying political and other criteria which relationships with citizens can be undertaken electronically.

This potential problem must also be assessed from a democratic perspective, taking into account the degree of satisfaction of the groups targeted by public services. Many citizens and businesses are increasingly getting accustomed to ICT tools in all other activities in an information society. Therefore, at least national, regional and medium/large local public administrations should adopt ICT-enabled solutions not only for their internal administrative activity – but also to give a better service to their citizens and customers.

Nevertheless, some inconveniences related to a wide recognition of the right to contact with public must be highlighted:

- Access to electronic public services is a too vague concept since it may mean many different things: access to information, to address application forms, to fulfil obligations, to complete some data… Therefore, the extent of the right to eAccess to public bodies may be quite different regarding each Public Administration and, as a last resort, it depends on its legal configuration according to the concrete circumstances of each public body[78].
- The legal recognition of a right to contact with bodies/authorities through electronic means should also be flexible but taking into account that sometimes some formal requirements have to be respected (i.e.: the submission of application forms, right to petition[79]…). From this perspective, the use of e-mail may be considered as a useful tool but it must be also taken into account that if no answer is given to citizens a serious risk of confidence —or even liability— can arise.
- Sometimes the recognition of a right is not the best way assure the use of electronic means. An example may be quite useful to explain the inconveniences of this perspective: if citizens have the right not to submit again electronic documents/information that are already in the hands of any Public Administration (articles 6.2.b and 9 Spanish Act 11/2007) it may occur that, due to a lack of confidence, they decide not to exercise their right and submit them in paper format. Therefore, a better solution is to forbid that public bodies demand those data/information to citizens and oblige them to share them through electronic means with a full respect to the requirements of data protection[80].

European-level considerations

The requirement outlined above is particularly relevant for the consolidation of certain essential principles at the European level. Among the most significant of these are administrative services linked to the free movement of persons and the right of establishment[81]. These services should be accessible through electronic means in order to allow their exercise in an effective way, according to the pressures and opportunities of the information society. This is particularly significant when a citizen must contact a public

[78] As an example, see the Dutch eCitizen Digital Charter. More information in deliverable 2 and at http://www.epractice.eu/cases/ecc

[79] Regarding this right, see http://www.epractice.eu/cases/epetitions

[80] For the respect of right to data protection in the field of eGovernment, please see the eProdat website at http://www.eprodat.org/

[81] These rights are established by Articles 39 (free movement) and 43 (right of establishment) of the EU Treaty.

administration located in a different Member State. If such services are not offered in an electronic version, it will be a paradox that most of the activities required (e.g. buying a plane ticket, renting a flat or opening a bank account) could be done using the Internet – but not those related to public administrations.

The relatively slow pace of many public administrations in Member States to offer high impact ePublic Services for citizens might be solved through legal changes which establish clear obligations that encourage innovation in this area. However, the final decision to offer a public service is mainly the responsibility of the relevant national and, even more, regional or local authorities. It cannot be always taken at EU level. If it is felt there would be a value in allowing decisions at the European level to force Member State authorities to supply at least the most useful of their services electronically, particularly for citizens, it would therefore be necessary to find an appropriate competence basis for such an EU-level intervention.

Public reports ranking the level of ePublic Services supply across Europe are an interesting method of reaching this goal, but their current methodology is not designed to address effectively the need for an electronic version of citizens' rights and freedoms. This means the establishment of legal eRights obligations at the European level should be considered as the most effective way to solve this barrier, although the particular circumstances of each country and the complexity of the services should be taken into account as essential conditions of particular decisions.

A relevant example here is the European initiative to promote, through Directives 2004/17/EC and 2004/18, the compulsory use of electronic means in the field of public procurement. Positive results from this obligation emerged rapidly in a number of Member States. For instance, France has not only adapted its own legal framework to meet these Directives' requirements but has gone even further than the Directives' recommendations.

More recently, and closely related to the recommended solutions we propose below, Directive 2006/123/EC on services in the Internal Market 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. This Directive has had a quick effect on the regulation of some Member States. For instance, the Spanish Law of 22 June on citizens' electronic access to public services has included specific digital rights (Article 6.3) regarding the administrative procedures establishing public services.

The Commission's (2006) eGovernment Action Plan i2010 highlights the importance of paying attention to citizen mobility services such as: improved employment mobility through online job search services across Europe[82]; social security services relating to patient records and electronic health prescriptions, benefits and pensions across Europe; and educational services enabling students to study in a Member State other than their home country. The use of electronic means should be considered as an excellent opportunity to reach this goal.

Although the supply of ePublic Services has considerably increased in recent years, there is still a need for going more deeply in the direction of putting eGovernment *au service du citoyens*, particularly at the European level. This is recommended, for example, by the European Economic and Social Committee (2006). To date, a significant administrative preference has been shown for those services addressed to companies rather to citizens (e.g. see Capgemini 2005). That imbalance can be explained by the way relationships between public administrations and companies are seen as essential to making the European market a reality by assuring open service provision.

Nevertheless, the democratic legitimacy of the EU depends on its activities taking a more citizen-centric perspective, in order to assure its citizens can exercise their rights and freedom in the most effective way. Increasingly, this is best carried out through electronic media.

[82] See Section 6 case studies in Deliverable 2.

Recommended solutions

We recommend the eRights issues highlighted here should be addressed through the approval of a new Directive on administrative services, linked to the free movement of persons and right of establishment. This should include the following (using Articles from Directive 2006/123/EC as a model, where relevant):

- Simplification of procedures (Article 4). Member States must examine their procedures and formalities for accessing public service activities. Where they are not simple enough, there should be an obligation to undertake appropriate streamlining.

- Right to information (Article 7). Detailed information is required to assist the obtaining of information in an appropriate form (e.g. the requirements applicable to providers of information established in a territory; contact details of the competent authorities; the means of, and conditions for, accessing public registers and databases on providers and services; the means of redress generally available in the event of dispute; and contact details of the bodies where practical assistance can be easily obtained through a single point, an obligation that will be fulfilled if all that information is accessible through electronic means). See also solutions recommended in this document in the sections on Privacy and Data Protection and Section 6 on Public Administration Transparency.

- Accessibility of procedures by electronic means (Article 8). Member States should have a clear and direct obligation to ensure all procedures and formalities concerning access to a public service activity and to the exercise thereof may be easily completed at a distance and by electronic means.

- Harmonization of administrative documents (Article 5.2). The Commission should be able to approve harmonized forms that will be considered equivalent to any document required of a provider of these services. Member States should also be made to accept any document from another Member State that serves an equivalent purpose as the certificate, attestation or any other document required to prove that a requirement has been satisfied.

- Better coordination among Member States. Improved Member State coordination should be encouraged, with a key aim of facilitating exchanges of the data required to obtain information through electronic means. A deeper collaboration would be also be required to allow the use of digital certificates supplied from a service provider established in a different Member State. Otherwise, a new obstacle would have been built.

Supporting multi-channel approaches to delivering and accessing public services, including the essential role of intermediaries

Why a multi-channel approach is needed to help bridge digital divides

As online public services have a long way to go before they are fully accessible and inclusive, legal issues relating to the accessibility of eGovernment services must be considered as a priority. However, reaching this objective could seem to be utopian for economic reasons (e.g. see European Commission 2004). For instance, efficiency requirements are leading to restrictions on access being applied to many eGovernment services being built across Europe, particularly in relation to administrative and legal information. This is exemplified by the way many official journals are edited only in an electronic version, at both at the national level (e.g. for Belgium[83]) and for regions and local authorities (e.g. for Catalonia[84]).

Nevertheless, the promotion of electronic public services cannot be focused on compulsory use of ICT by citizens because that kind of measure may infringe the principle of equity in the

[83] See: http://www.moniteur.be

[84] See: http://www.gencat.net/dogc/cas

access of users to public services. Instead, as highlighted by Centeno et al (2004), one of the main legal requirements in this field is “the need to find the balance between a harmonized framework and mandatory legislation”. Moreover, this option can be considered fair – and sometimes constitutional – only if no unjustifiable limitations are placed on the exercise of citizens’ and companies’ rights or the fulfilment of their obligations.

The existence of a digital divide that affects a wide range of groups in several Member States makes it essential to guarantee access to public services regardless of the channel chosen by citizens. The use of at least two channels (one electronic, one more traditional) to gain access to public services should be guaranteed as a rule to avoid discrimination since “if a user is legally entitled to a service, the administration is legally required to deliver the service” (European Commission 2004).

In order to ensure no citizen is left behind in moves towards eGovernment, the provision of a multiple-channel choice should be recognized as the preferable approach. But this option is not always feasible, due to problems such as financial constraints and the difficulties of managing documents in more than one format. Other solutions must therefore be sought to promote the innovative use of ICTs as a tool to incorporate socially disadvantage groups, as outlined by the European Commission’s (2006) eGovernment Action Plan. This demands a new perspective to deal with obstacles to the inability or impossibility of some disadvantaged groups to access public services electronically.

Policy making constraints at EU level

General and direct solutions at a European level cannot be adopted since the practical conditions for the accessibility of ICT-enabled services are different in each Member State, and for each group of users. For instance, access problems can range from those related to the physically disabled, to situations where access is too difficult for technical reasons or the failure to respect technological neutrality has made it impossible to use an electronic service without certain software or equipment that may not be readily available.

Serious attempts to overcome these problems would be assured if public administrations had clear legal accessibility obligations, although as a last resort each public body must solve its inconveniences in a way appropriate to its own requirements. European authorities with a wide competence in the field of public procurement should be required to observe a stricter respect in ePublic Services of the provisions in Directives 2004/17/EC and 2004/18/EC referring to the inclusion of persons with disabilities and older people.

European-wide solutions are also constrained because a strong and general harmonization is not possible in this field. EU competence is established only where fundamental rights and freedoms are concerned, as happens with public procurement. But this is unlikely to be applicable in relation this legal area. In addition, concrete social, economical, cultural and technological circumstances in each Member State – and, even more, at the regional and local levels – lead to different requirements and decisions in different contexts. An important point to note is that EU formal documents on eGovernment can recommend the use of alternative systems based on the collaboration of certain intermediaries who have a close relation with those social groups affected by digital divides.

Recommended solutions

Despite the constraints at EU-level outlined above, we can make some specific recommendations. Directives 2004/17/EC (Article 34 and Annexe XXI) and 2004/18/EC (Article 23 and Annexe VI) have established clear obligations for public Administrations to include technical specifications in contract documentation. A stronger observation of the compliance of these provisions by Member States (at national, regional and local level) in eGovernment developments would be of great benefit in addressing digital divides because it would help to widen the range of choices available, such as for the disabled.

A formal recommendation should therefore be made by EU authorities to Member States to ask them to recognize the need to fight against digital divides by assuring access to eGovernment services for groups with a range of social and economic difficulties. This can be achieved by, for example, offering multiple online and offline choices to promote social inclusion. An emphasis should also be given to the valuable role that could be played by intermediaries and representatives who can assist citizens to gain access to online services[85].

These recommendations could follow the criteria used by the EU's Inclusive eGovernment Ad Hoc Group (2006) in identifying relevant stakeholders, including: social intermediaries; private sector actors; civil servants and other public service agencies; and Non-Government Organizations (NGOs). Member States should be urged to adapt their general legal framework governing citizens' representations to public administrations to include electronic requirements. Key issues to address in this respect are: the use of digital signatures (see also Section 2 on Authentication and Identification); the conditions and limits of each sort of relationship; and proof of citizens' consent. Unless such legal adaptations are made in an effective way, there could be serious risk that citizens' trust in eGovernment will be undermined because of fears about liability and related issues (see also the section in this document on liability).

References

Publications

Capgemini (2004), Online Availability of Public Services: How is Europe Progressing? Report of the Fourth Measurement October 2003, Brussels: European Commission, Directorate General for Information Society and Media, http://europa.eu.int/information_society/eeurope/2005/doc/highlights/whats_new/capgemini4.pdf

Capgemini (2005), Online Availability of Public Services: How is Europe Progressing? Report of the Fifth Measurement October 2004, Brussels: European Commission, Directorate General for Information Society and Media, http://ec.europa.eu/information_society/soccul/egov/egov_benchmarking_2005.pdf

Centeno, C., van Bavel, R. and Burgelman, J-C. (2004), eGovernment in the EU in the Next Decade: The Vision and Key Challenges, Technical Report EUR 21376, Brussels: Institute for Prospective Technological Studies (IPTS), European Commission, http://europa.eu.int/idabc/servlets/Doc?id=19131

European Commission (2004), Multi-channel Delivery of eGovernment Services, Brussels: European Commission, Enterprise Directorate-General, http://ec.europa.eu/idabc/servlets/Doc?id=16867

European Commission (2005), CoBrA Recommendations to the eEurope Advisory Group, Brussels: European Commission, DG Information Society, eGovernment Unit, http://ec.europa.eu/idabc/servlets/Doc?id=18465

European Commission (2006), i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, Brussels: European Commission, http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/egov_action_plan_en.pdf

European Economic and Social Committee (2006), Opinion of the European Economic and Social Committee on the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: i2010 eGovernment Action Plan — Accelerating eGovernment in Europe for the Benefit of All, COM(2006) 173 final, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/c_325/c_32520061230en00780081.pdf

Inclusive eGovernment Ad Hoc Group (2006), i2010 eGovernment subgroup, Analysis of European Target Groups Related to Inclusive eGovernment, http://ec.europa.eu/information_society/activities/egovernment_research/doc/analysis_of_european_target_groups.pdf

[85] See the section on Relationships in deliverable 1b for more background to these issues.

EU-level, national and other relevant legislation and regulations

Directive 2004/17/EC of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors, Official Journal of the European Union, L 134, 30/4/2001, pp. 1-113, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

Directive 2004/18/EC of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, Official Journal of the European Union, L 134, 30/4/2001, pp. 114-240, http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en01140240.pdf

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

Spanish Act 11/2007 on citizens' electronic access to public services, http://www.epractice.eu/document/3677

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

Re-use of Public Sector Information

Professor Cécile de Terwangne and Dr Cristina Dos Santos

Centre de Recherches Informatique et Droit (CRID), University of Namur, Belgium

Introduction

Directive 2003/98/EC on the re-use of Public Sector Information (the ‘PSI Directive’) defines ‘re-use’ as the use by persons or legal entities of documents held by public sector bodies for commercial or non-commercial purposes, other than for the initial purpose related to the public task for which the documents were produced.

The PSI Directive is important because several eGovernment services depend on such re-use. However, it does not eliminate all obstacles to the desirable re-use of PSI and the establishment of a pan-European public information market. For example, Member States and their public bodies are left to decide whether or not to allow such re-use in particular circumstances. Implementations of PSI re-use systems also vary between Member States and between different governance levels within a nation, as they depend on the specific access regimes in Member States.

A number of practical issues mean that provisions for PSI re-use can benefit or disadvantage different sections of society, thereby bridging or exacerbating digital divides. For instance, the PSI Directive’s imprecise reference to a “reasonable return of investment” when fixing charges for the re-use of public documents could lead to differences in the costs for citizens and business in different contexts. The formats in which documents are provided can also be more difficult or easier to handle by different users depending on the resources and skills at their disposal. Availability in appropriate languages and the ease of finding documents are other significant digital divides’ aspects of this legal issue.

The way the PSI Directive leaves detailed regulation on re-use to Member States and their public bodies makes it limited as a tool for coordinating regulation in this area, including no clear elucidation on the principle of whether re-use itself should be allowed. The lack of a PSI re-use culture in most Member States can also lead to blockages in workplace and organizational processes and structures when they need to be adapted to take account of eGovernment initiatives.

In the relatively underdeveloped market of environmental information, for example, obstacles are often caused by public administrations who are not accustomed to locating appropriate information in an easily accessible form or to negotiating with the private sector where necessary. Moreover, some public sector documents are excluded from the scope of the PSI Directive, such as those for which third parties hold the Intellectual Property Rights (IPR). More generally, the Directive has not solved the problem of divergences of national legal regimes regarding IPR or data protection (see relevant sections in this document). Contentions about competition between public and private interests regarding electronic data also need to be resolved, for instance when a government department is tempted to exploit its information to increase its revenue.

Below we propose possible solutions to overcome remaining barriers identified in our previous legal analysis of this area in Deliverable 1b.

Enhancing adherence to the PSI Directive’s text and fostering a PSI re-use culture

There are problems in the degree to which national laws respect the text of the PSI Directive (e.g. see European Commission 2007). For instance, Forster (2007: pp. 6–9) has argued that there are “historical barriers to PSI exploitation”, noting that even if “some organizations claim that the PSI Directive has led to ‘bureaucracy’, those concerned should check whether this is not the result of inadequate transposition or of the way in which the organization had been handling its data historically.” Forster also emphasizes that “no complications whatsoever are inherent in the Directive (…) but it needs to be correctly transposed”.

Recommended solutions

Actions by the European Commission

The EC has already taken diverse actions to stimulate a good transposition of the PSI directive (creation of the PSI Group and organisation of meetings of this group). But divergences of implementation at the State level still remain.

The PSI Expert Group was set up by the Commission in 2002. It consists of Member State officials, local or regional authorities, representatives from private sector organizations and consumer organizations. In principle, it meets twice a year to exchange good practices of PSI re-use, share experiences of initiatives supporting PSI re-use and other practical issues regarding implementation of the PSI Directive. As the transposition of the PSI Directive provisions has largely been completed in most Member States, the focus of the Group's discussions has moved towards ways of maximizing impacts of the Directive in practice[86].

We suggest that PSI re-use authorities be created at national level either spontaneously by the Member States (see hereunder) or on a compulsory way by an initiative taken at the EC level (through the review of PSI Directive, for example). Actions of these authorities could be coordinated at a pan-European level by the PSI Expert Group[87]. This could be the right solution for increasing awareness of the opportunities made possible by the re-use of PSI and the greater harmonization of these activities within the EU. It could also help to overcome the lack of trust in this field. The Article 29 Working Party in the data protection field could be a model to reinforce the Group's role and competences (see also the section on Privacy and Data Protection in this document).

We also propose that the PSI Expert Group should be given more authority to monitor and eventually 'punish' or otherwise enforce[88] decisions in Member States that have committed themselves to respect its opinions on PSI re-use.

One way of achieving coordination is pointed to by the recent Directive 2007/2/EC on establishing an Infrastructure for Spatial Information in the European Community (INSPIRE). This aims to assist sharing the use of spatial data and associated services between public authorities for the performance of public tasks. A similar implementation process could also be applied to the re-use of PSI more widely. As this is a framework Directive, the detailed technical provisions would be laid down in Implementing Rules (IRs), for submission to the relevant Committee in a process known as 'comitology'[89]. Once agreed, IRs will be published as a Regulation that is automatically and directly binding for Member States. The INSPIRE Directive also has relevant exemplars pointing to appropriate monitoring and reporting mechanisms that could be applied in cost charging and data sharing policies.

If a Member State is deemed to have violated its Treaty obligations, the EC could also pursue an 'infringement procedure' to attempt to persuade the Member State to comply with Community legislation. This has had some positive results in the past[90]. Nevertheless, as Forster (2007: 19–21) stresses: "A legalistic transposition of the Directive is in itself not enough to bring out the full potential of public sector information for the European economy and society. The deployment of further implementing and facilitating measures is highly

[86] This focus on maximizing the impact was highlighted at the 9th Meeting of the Expert Group on 28 November 2006 by Javier Hernández-Ros, Head of the Digital Libraries and Public Sector Information Unit, Information Society and Media DG, European Commission.

[87] See: http://ec.europa.eu/information_society/policy/psi/psi_group/index_en.htm

[88] An example of current enforcement procedures is indicated by the first complaint procedure in the UK involving the Ordnance Survey, the UK Mapping Agency (see: http://www.opsi.gov.uk/). In the UK, decisions of the Office for Public Sector Information (OPSI) are not formally legally binding for public sector bodies, such as Ordnance Survey, as any of the parties in a complaints procedure could appeal against its decisions and can pursue the matter through the Courts.

[89] 'Comitology' is a procedure established by Article 202 of the EC Treaty allowing the creation of committees that act as forums for discussion. These consist of representatives from Member States and are chaired by the Commission, enabling it to establish a dialogue with national administrations before adopting implementing measures. The Commission ensures that such measures reflect as far as possible the situation in each of the countries concerned. (For more on comitology see: http://europa.eu/scadplus/glossary/comitology_en.htm).

[90] Article 226 of the EC Treaty empowers the Commission to put in place this infringement procedure.

desirable". In 2006 this infringement procedure was used against five Member States: Austria, Belgium, Portugal, Spain and Luxembourg – Belgium subsequently adapted its implementation law (see Belgian Law of 7 March 2007 relating to Directive 2003/98/CE, http://www.ejustice.just.fgov.be/doc/rech_f.htm).

The EC could continue to undertake assessment studies in specific sectors of great interest to have a correct view of the way the PSI Directive is respected in these sectors. That was done for example with the 'call for tenders' of 27 June 2007 regarding the geographical, meteorological and legal information sectors[91].

In this context, we also support the pursuit of the EC policy favouring co-funding of projects that aim to demonstrate the potential of PSI re-use at local, national and pan-European levels.

Finally, the EC should go on with the stakeholders discussions organized in the framework of the ePSIplus Thematic Network about the categories of information exempted from the PSI Directive scope.

Actions by the Member States

We support the recommendations of the ePSIplus Thematic Network (e.g. see ePSIplus 2007a, b). This includes an emphasis on "the need for pro-active action to be taken by Member State lead public bodies to assist the public sector as a whole to implement and comply with the PSI framework in a cost effective manner (whether with full compliance of the PSI Directive, or by enforcing compliance of decisions following complaints in a timely manner, for instance)"[92.]

In the same sense, Member States should implement a transparent policy regarding re-use of PSI that respects relevant provisions of the PSI Directive, such as those regarding the availability of formats (Article 5), transparency (Article 7) and non-discrimination and fair trading (Articles 10 and 11).

As noted above, it would be useful to create an independent national PSI authority in each Member State (such as the UK's OPSI, the Office of Public Sector Information[93]) whose action would be coordinated at the European level.

Moreover, to tackle the leadership failure and foster re-use culture inside public sector Member States could

- designate persons endorsed with decision power in this matter
- designate officials to consider the implementation of PSI re-use rules
- constitute expert groups to exchange about good practices

This solution follows the model of the European Commission's (2006) Decision to give power to its Directors-General and Heads of Service to take decisions in this field, including to "designate an official to consider applications for re-use and coordinate the response of the Directorate-General or Service". Article 11 of this Decision also permits the constitution of an "inter-service expert group" for an exchange of good practices inside the European Commission itself.

Removing disparities between Member States in charges for PSI re-use

The PSI Directive authorizes charges for the costs of "reproduction and dissemination", as well as costs of "collection and production" of documents. Article 6 of the Directive states: "where charges are made, the total income from supplying and allowing re-use of documents shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment". This could lead to a rapid increase in costs of access for the private sector in some crucial fields (e.g. in the meteorological sector in Finland),.

[91] For up to date information on such projects, see: http://ec.europa.eu/information_society/policy/psi/index_en.htm.
[92] See: http://www.epsiplus.net/epsiplus/news/newsletter/epsiplus_update_no_2.
[93] See: http://www.opsi.gov.uk/

At the same time, the Directive is rather contradictory about this issue, as its Recital 14 states: "(…) Member States should encourage public sector bodies to make documents available at charges that do not exceed the marginal costs for reproducing and disseminating the documents [authors' emphasis]". This is the solution already adopted by, for instance, the European Commission (2006) in its Decision of 7 April on the re-use of Commission information.

Article 7(1) of this Decision states: "the re-use of documents shall in principle be free of charge" and, in specific cases, "marginal costs incurred for the reproduction and dissemination of documents may be recovered". Article 7(3) also makes it clear that only excessive costs of adaptation should be charged and that the costs of collection and production should not be included: "In cases where the Commission decides to adapt a document in order to satisfy a specific application, the costs involved in the adaptation may be recovered from the applicant. The assessment of the need to recover such costs shall take into account the effort necessary for the adaptation as well as the potential advantages the re-use may bring to the Communities (…)". The provisions in this Commission Decision go well beyond the Directive in the field of charging, where only "marginal costs of dissemination" are allowed.

Finally, the reference to a 'reasonable return on investment' that can be included in the costs claimed to the re-users is vague and asks for precision.

Recommended solutions

Actions by the European Commission

The EC should see to undertake a pan-European discussion with all stakeholders

- to clarify the means and conditions of establishing whatever costs are to be charged,
- in particular in defining what is meant by a "reasonable return on investment".
- This discussion should take into account the differences of costs between commercial and non commercial re-use[94], including the way to determine both, in order to avoid discriminations and unfair competition between the private sector and public administrations.

This has already been partially done by the PSI Expert Group and could be further conducted by way of the ePSIplus Thematic Network[95], which is supporting the implementation of the PSI Directive in the period leading up to its review in 2008 and seeking to raise further awareness among stakeholders of this upcoming review.

Establishing re-use as an obligatory principle and clarifying the scope of public tasks

A main barrier mentioned in Deliverable 1b is that the PSI Directive leaves to the Member States and their public bodies the determination of whether or not to allow the re-use of PSI. Where it is not allowed, the Directive has no application. This option emerged as the result of political discussions between Member States during the formulation of the Directive. Member States' perceptions of their interests related to such re-use (valued at €10 to €48 billion in the

[94] For instance, this was done within the framework of the European Commission's (2006) Decision that concluded (Rantala 2006), "the EU Publications Office (EurLex) and Eurostat issue licenses only in specific cases of commercial re-use and can charge for it when a re-user asks for a special service (e.g. EurLex)".

[95] See http://www.epsiplus.net/epsiplus for details of the activities of ePSIplus and the events it organizes. This Thematic Network provides a 'one-stop shop' on re-use of PSI at the European level through a portal that opens access to a wide range of knowledge of key interest to many public and private sector stakeholders, including the opportunity to engage in debate on key issues in thematic and national workshops across EU Member States. It is funded by the eContentplus programme (see http://ec.europa.eu/information_society/activities/econtentplus/index_en.htm). .

EU[96]) vary according to the diverse political and historical influences, and organizational processes, within different public sector contexts.

Whereas certain Member States prefer to leave to each department or puboic body the choice of allowing re-use or not, others establish re-use as an obligatory principle. For example, the European Commission Decision of 7 April 2006 asserts the "re-use principle" as a sort of 'eRight of re-use'. Article 4 of the Decision requires that "all documents shall be re-usable for commercial or non-commercial purposes"[97] as part of a process aimed at encouraging "the availability of documents through electronic means where possible".

Recommended solutions

Actions by the European Commission

We suggest it could be opportune to review how far, if at all, the positions of Member States have evolved towards a point at which Directive 2003/98/EC could be amended to make re-use as a fundamental obligatory principle for all. This would, of course, require a list of restrictions or exceptions that Member States could use to protect some 'national interests', for example to safeguard the economic viability of a specific public service that warrants such a provision.

In principle, public administrations in many Member States are not bound by private sector laws, such as competition rules. This is because such laws have not generally applied to the administration's primary functions, and they have their specific field of law (see also Section 1 on Administrative Law). However, public administrations increasingly compete with the private sector in many fields. The 'principle of non-discrimination' in Article 10(2) of the PSI Directive already states: "If documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the documents for those activities as apply to other users". Anyway, there is still a lack of a clear common definition about what is or not a "public task" (and therefore what the commercial activities are "which fall outside the scope of its public tasks"[98]).

We recommend therefore establishing a global policy through discussions by national experts at a pan-European level, in order to provide clear guidance to national PSI holders. Such discussions could aim at addressing the question of determining what a public task is and what goes beyond it, by focusing on specific fields of activities. This would lead to a determination field by field, for example for commercial registers, legal data, geographical data (see Directive INSPIRE above-mentioned), meteorological data,… A framework allowing recurrent review of the defined scope of these public tasks should be set up.

Addressing potential IPR and data protection obstacles

Important barriers to re-use remain in relation to IPR issues (see also solutions proposed in this area in Section 3) and data protection requirements (see also Section 5). These could be overcome by adopting an EU-wide 'global vision' of re-use possibilities and risk assessments. However, within a global vision about eGovernment, the Commission should bear in mind data protection requirements when re-using information containing personal data, namely that: "extreme care must be taken in not infringing personal rights just because of convenience or (fair and respectable) economic interests"[99].

[96] According to the European Commission's MEPSIR project studying the effects of the PSI Directive on re-use in Member States (see MEPSIR 2006 and http://www.mepsir.org).

[97] Save for some explicit exceptions in Articles 2(2) and 2(3),

[98] For instance, many stakeholders at an ePSIplus Thematic Meeting (2007) highlighted the fact that public administrations used this notion of "public task" as a way of rejecting unilaterally and powerfully re-use requests (especially in the meteorological information sector).

[99] Personal communication from our Project's Expert, Mr. Emilio Aced Félez, Head of the Inspection Unit, Data Protection Agency of Madrid, Spain (www.apdcm.es).

Recommended solutions

Actions by Member States and public sector stakeholders

Public bodies hold personal data because their collection is compulsory through the application of different national regulations or are requested when citizens make a claim or ask for any service. This implies that the data collection process used by public bodies often include occasions where there is no room for the consent of individuals. It is therefore important to maintain the rights of citizens as 'data subjects', as provided by Directive 95/46/EC (e.g. the "right of information" and the "right of access" specified in Article 10 and following of the Directive).

There is no formal hierarchy between European Directives. Stakeholders must respect the aim of trying to achieve the 'right' balance between the different interests at stake in the eGovernment field.

Overcoming practical and technical barriers

Practical and technical barriers yet to be resolved include:

- language diversity, which could raise particular problems of costs when wider access to PSI is viewed from a cross-border perspective;
- developing and successfully implementing effective tools to identify the availability of public sector documents, such as through the availability of 'meta-data' overview guides to help identify and find information; and
- the lack of common standards for storing public sector information.

Recommended solutions

Actions by the European Commission

The expansion of the EU, in mid-2007 with 27 Member States and 20 different languages, means a strategy should be developed to create policies to deal effectively with such practical issues. Semantic research could help to deal with the diversity of languages challenge, even if it won't represent a complete solution.

As in the previous PSI re-use solutions, we emphasize the need to have more standards at a pan-European level, especially to enable re-use across borders. The EC should organize discussions at European level to adopt standards, notably on these crucial points: standard formats for storing documents and standards to elaborate meta-data guides. The meta-data guides should at least indicate: an identification of the documents or categories of documents available for re-use, their format, their location, the conditions and charges for re-use (if any), the body responsible to allow the re-use or to give a license (if any).

Actions by the Member States

We also recommend that Member States should opt for a clear policy regarding re-use of PSI at their national level. This should aim to help stakeholders put in place a more harmonized 'minimum set of rules', as already provided by the PSI Directive.

Member States should take part to the European discussions concerning standards.

References

Publications

ePSIplus (2007a), Public Sector Information: A collation of country reports provided by the Thematic Network Partners, V2.1, 24 February 2007, http://www.epsiplus.net/epsiplus/media/files/epsiplus_countryreports_24feb07_v2_1 ePSIplus (2007b), Public Sector Information: Financial impact of the PSI Directive – Pricing and Charging Key Issues – An overview, V2.0, 15 April 2007, http://www.epsiplus.net/epsiplus/media/files/epsiplus_pricingintroduction_v2

ePSIplus Thematic Meeting (2007), PSI Pricing 1: Impact Analysis in the Context of the PSI Directive, Helsinki, 19-20 April 2007, http://www.epsiplus.net/epsiplus/events/epsiplus_thematic_meetings/financial_impact_thematic_meetings/psi_pricing_1_impact_analysis_in_the_context_of_the_psi_directive

European Commission (2006), Decision of 7 April 2006 on the re-use of Commission information, (2006/291/EC, Euracom), Official Journal of the European Communities L107, 20.4.2006, p.38, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_107/l_10720060420en00380041.pdf

European Commission (2007), Implementation of the PSI Directive: Implementation status in Member States, http://ec.europa.eu/information_society/policy/psi/actions_ms/implementation/index_en.htm

Forster H. (2007), Public Sector Information: A Motor for Growth and Employment, International Symposium on ‘Public Data in the Private Market: New regulations on the Re-Use of PSI’, Potsdam, 4 June, http://ec.europa.eu/information_society/policy/psi/docs/pdfs/potsdam_symposium/speech.pdf

MEPSIR (2006), Final Report on Study on Exploitation of PSI – benchmarking of EU framework conditions, June, http://www.epsiplus.net/epsiplus/reports/mepsir_measuring_european_public_sector_resources_report

Rantala, M. (2006), Minutes of the 9th Expert Group Meeting, Presentation of Commission Decision 2006/291/EC, EURATOM, on the Re-use of Commission Information, Brussels: European Commission, http://ec.europa.eu/information_society/policy/psi/docs/pdfs/minutes_psi_group_meetings/9th_28_november_2006.pdf

EU-level, national and other relevant legislation and regulations

Belgian Law of 7 March 2007, Loi du 7 mars 2007 transposant la directive 2003/98/CE du Parlement Européen et du Conseil du 17 Novembre 2003 concernant la réutilisation des informations du secteur public, http://www.ejustice.just.fgov.be/doc/rech_f.htm)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281, 23.11.95, pp. 31-50, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf; http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, Official Journal of the European Communities L 345, 31/12/2003, pp. 90–6, http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_345/l_34520031231en00900096.pdf

Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), Official Journal of the European Communities L 108, 25/4/2007, pp. 1–14 (entered into force on 15 May), http://www.ec-gis.org/inspire/directive/l_10820070425en00010014.pdf

Section 5: Conclusion

The Internet and related electronic information and communication technologies (ICTs) are being used increasingly in Europe to enhance the delivery of public services and citizens' democratic engagements with government. However, many eGovernment innovations that could benefit all citizens have been hampered by legal, organizational and other obstacles.

The research from the Breaking Barriers project has demonstrated that there are no simple 'single-bullet' solutions for defeating the obstacles to effective eGovernment across Europe. On the contrary, the barriers to eGovernment are multiple, interrelated and resistant to change. Thus in this report the team have proposed at least one organisational solution for each barrier category and at least two legal solutions for each legal area. The team was not, therefore, aiming to produce solutions to all the potential problems of eGovernment, but to identify a range of tangible solutions to specific barriers.

At a general level, there are overriding themes that have emerged from this work. The first concerns the centrality of organisational innovation to eGovernment. The use of ICTs in government should not be based on a media-substitution paradigm where ICTs merely automate aspects of existing practices. What is required instead is network-enabled transformation where ICTs are used to transform government. Such change requires fundamental innovation in the workplace. For this reason, the EC must develop policies in order to facilitate such e-enabled organisational change.

Examples of organisational solutions arising from the research include: creating a network of eGovernment champions, working with chaotic co-ordination and encouraging an literate workforce. Each of these offer a solution to address some of the most significant barriers to eGovernment: coordination across central, regional and local levels of government; resistance to change by government officials; lack of interoperability between IT systems; and lack of political support for eGovernment.

Secondly, in relation to legal barriers, there are many complex and related issues across a range of arenas. However, there is a growing sense that the law can be harnessed to enable rather than constrain eGovernment, such as by establishing the digital rights of citizens. By forcing governments to permit citizens to use eGovernment, policy can overcome continuing digital divides and enable all citizens to benefit from the effectiveness gained by transforming eGovernment

Examples of legal solutions discussed include improving co-ordination in authentication and identification activities, ensuring liability does not undermine trust in eGovernment, overcoming disparities in the implementations of the Data Protection Directive and establishing an eRight for citizens to use electronic media to access public services. These solutions are designed to overcome key barriers within the fields of authentication and identification, liability, privacy and data protection and relationships between public administrations, citizens and other ICT actors respectively.

It is worth noting that some of the solutions put forward could be used to tackle more than one barrier. For example, giving sustained attention to eGovernment issues by creating a network of Chief Information Officers is also likely to engender cultural change, a good way to tackle workplace inflexibility. In this way, implementation of the proposed solutions can reinforce each other and have a generalised effect in promoting IT-enabled business change across a range of government activities.

We hope that these recommendations are considered in order to further the objectives of the European Commission's i2010 eGovernment Action Plan: leaving no citizen behind; making efficiency and effectiveness a reality; implementing high-impact key services for citizens and businesses; putting key enablers in place; and strengthening participation and democratic decision-making that were reinforced by the Lisbon Ministerial Declaration of the 19th of September 2007.

The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

Prepared by:

Rebecca Eynon
Project Manager
Oxford Internet Institute
University of Oxford
1 St Giles
Oxford OX1 3JS

For further information about the eGovernment Unit

European Commission
Information Society and Media Directorate-General
eGovernment Unit

Tel (32-2) 299 02 45
Fax (32-2) 299 41 14

E-mail EC-egovernment-research@cec.eu.int
Website europa.eu.int/egovernment_research