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

A Legal and Institutional Analysis of Barriers to eGovernment

Draft Deliverable 1b

16/08/2006

ACKNOWLEDGEMENTS

The Breaking Barriers project team would like to thank all the members of the expert group for their valuable thoughts and comments that have helped to shape this document. They are:

- **Albena Kuiumdjieva**, Executive Director, Law and Internet Foundation, Bulgaria
- **Albert Jacob Meijer**, Assistant Professor at the Utrecht School of Governance, Netherlands
- **Alexandre Caldas**, Director of CEGER (the Management Centre for the Government Electronic Network), Portugal
- **Ari-Veikko Anttiroiko**, Adjunct Professor, Department of Regional Studies, University of Tampere, Finland
- **Dariusz Bogucki**, Ministry of Science and Information Society Technologies, Poland
- **Derrick Pisani**, Central Information Management Unit, Office of the Prime Minister, Malta
- **Elise Debies**, ADAE Agence pour le développement de l'administration électronique, France
- **Emilio Aced Félez**, Representative from e-PRODAT (Best practices in Data Protection and e-Government in Europe), Spain
- **Fernando Galindo**, Universidad de Zaragoza, Spain
- **Francesco Bolici**, LUISS Guido Carli University, Rome, Italy
- **Gloria Cassar**, Business Development Manager, Malta Information Technology & Training Services Ltd, Malta
- **Manuel Baptista**, Consultant, eGovernment Observatory, Belgium
- **Mikkel Hemmingsen,** Ministry of Science and Technology, Denmark
- **Jens Hoff**, Department of Political Science, University of Copenhagen, Denmark
- **John Shaddock,** Yorkshire and Humber Assembly, Wakefield, UK
- **Juliet Lodge,** Director of the Jean Monnet European Centre of Excellence (JMECE), University of Leeds, Leeds, UK
- **Miriam Lips**, Associate Professor, Center for Law, Public Administration and Informatisation, University of Tilburg, Netherlands
- **Mirko Vintar**, Chair for Informatics & Organisational Sciences Faculty of Public Administration, University of Ljubljana, Slovenia
- **Panos Hahamis**, Senior Lecturer, Business Information, Management and Operations, Westminster Business School, UK
- **Paul M.A. Baker**, Georgia Centers for Advanced Telecommunications Technology (GCATT), USA
- **Raj Kumar Prasad**, CEO, Institute for Electronic Governance & Development, Centre for e-Governance, New Delhi, India
- **Rey Koslowski**, Associate Professor of Political Science, University at Albany (SUNY), USA
- **Rosario Osuna Alarcón**, Professor of Information Science, Salamanca University, Spain
- **Steve Hodgkinson**, Deputy CIO, Office of the Chief Information Officer, Victoria State Government, Melbourne, Australia
- **Steve Sawyer**, Associate Professor, College of Information Sciences & Technology, The Pennsylvania State University, Pennsylvania, USA

- **Tatjana M. Zupan**, Ministry of Public Administration, Slovenia
- **Tom Van Engers**, Professor in Juridical Knowledge Management, University of Amsterdam, Netherlands

PREFACE

This is a 'work in progress' report on the goals, initial findings, plans and background of the European Commission's *Breaking the Barriers to eGovernment* project[1], which began in January 2005. It highlights how results from investigations in the project's first phase, including an online survey, are helping to clarify the most significant legal and organizational impediments to fulfilling the EU's eGovernment goals. This includes the initial identification of seven key types of barrier and the main legal foundations that can significantly facilitate or block successful eGovernment outcomes. Feedback[2] on the interim results presented here will be combined with further detailed studies and analyses to refine and develop the project's findings for our final report in December 2007.

There are five parts to the document.

- Part 1 is an executive summary that outlines: the project's aims; the key goals of eGovernment in the EU; the project's approach to investigating barriers to achieving these goals; and the key barriers and related legal issues identified at this stage. It also indicates the relative importance of barriers and their legal dimensions.

- Part 2 summarizes the project team's view of the two main topics being investigated: the most significant categories of eGovernment barriers and the main legal dimensions to these blockages.

- Part 3 discusses the methods employed in the project's investigations: a systematic review and analysis undertaken by the team's specialists; a recent online survey; plans for case studies; and ongoing consultations with stakeholders and expert workshops. The set of research questions guiding this work are also illustrated in this part.

- Part 4 has papers by specialists among the project's partners that analyse in detail the main legal foundations underpinning the barrier categories discussed identified in Part 2. These cover eight prime legal dimensions: 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; and re-use of public sector information.

- Part 5 contains references giving details of research and literature sources examined by the project team.

[1] This project (see http://www.egovbarriers.org) is part of the Commission's MODINIS research programme (http://europa.eu.int/information_society/activities/egovernment_research/projects/i2010_studies/index_en.htm).
[2] Contact details are available at http://www.egovbarriers.org

PART 1: EXECUTIVE SUMMARY

Background

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 [3]. 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"[4].

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[5,6,7,8]. Substantial legal, political, administrative, social, institutional and cultural differences between Member States and regions[9,10] in the EU make such understanding of the main impediments to eGovernment of particular relevance to the growing number of important public services in the EU that seek to span national and regional boundaries (e.g. eProcurement for cross border public tenders and support for employment mobility). New initiatives are also often needed when rapid technologically-enabled change creates problems by outpacing the evolution of legal and organizational arrangements.

The study reported here is therefore of particular importance because, as its title explains, it is seeking ways of 'Breaking Barriers to eGovernment'[11]. Its aims in doing this are to:

- Create awareness of potential policy and practical barriers to successful eGovernment within the EU and its Member States.

- Undertake detailed eGovernment case studies, survey research and other focused investigations to gather evidence in different contexts and from many

[3] European Commission (2003), The Role of eGovernment for Europe's Future, COM(2003) 567, available at, http://europa.eu.int/information_society/eeurope/2005/doc/all_about/egov_communication_en.pdf
[4] European Commission (2002), Communication on eEurope 2005: An Information Society for All, available at, http://europa.eu.int/information_society/eeurope/2005/all_about/action_plan/index_en.htm
[5] European Commission (2003), The Role of eGovernment for Europe's Future, SEC (2003) 1038, available at, http://europa.eu.int/information_society/eeurope/2005/doc/all_about/egov_communication_en.pdf
[6] OECD (2003), The eGovernment Imperative, available at, http://Webdomino1.oecd.org/COMNET/PUM/egovproWeb.nsf/viewHtml/index/$FILE/EGovernment%20Imperative%20Final().pdf
[7] Australian Government Information Management Office (2003), EGovernment Benefits Study , available at, http://www.agimo.gov.au/publications/2003/03/e-govt_benefits_study
[8] Institute for Prospective Technological Studies (2004), eGovernment in the EU in 2010: Key Policy and Research Challenges – Workshop Report. European Commission , JRC, Seville, Spain, August
[9] Leitner, C. (2003), e-Government in Europe: The State of Affairs, available at, http://www.e-europeawards.org/view_extern.asp?id=4706
[10] Graafland-Essers, I. and Ettedgui, E. (2003), Benchmarking E-Government in Europe and the US, available at, http://www.rand.org/publications/MR/MR1733/MR1733.pdf
[11] The MODINIS programme, of which this project is a part, is examining four areas eEurope 2005 implementation: monitoring and comparison of performance; dissemination of good practices; analysis and strategic discussion; and improvement of network and information security.

stakeholders to help identify and explore the most significant eGovernment barriers and their associated institutional and legal underpinnings.

- Develop guidance on productive initiatives and solutions with a European dimension that could avoid or remove blockages to eGovernment progress in Europe, including a set of best practice recommendations.

- Build a rich and informative online inventory of issues that are of significance to eGovernment take-up.

- Engage a broad group of legal experts and eGovernment practitioners through a comprehensive outreach and consultation programme.

The remainder of this part summarizes the main elements in the project: the key eGovernment goals whose achievement could be hampered by the barriers identified; the methods used by the project team in its investigations; the seven key barrier categories we have identified; and the main legal issues examined in depth by the team's specialists.

Key European eGovernment Goals

For this project, 'successful eGovernment' broadly means the achievement of five prime EU-level objectives[12]:

- *No citizen left behind*[13]. All citizens, including socially disadvantaged groups, should be major beneficiaries of eGovernment. To meet this inclusivity aim, European public administrations need to make public information and services more easily and cost-effectively accessible through innovative uses of ICT. Achieving this goal also crucially requires greater public's awareness of, and trust in, eGovernment services and their benefits, together with the development of appropriate skills among all citizens.

- *Making efficiency and effectiveness in public services a reality*. High user satisfaction with public services should be established by using ICT innovations appropriately to reduce the administrative burden on citizens and businesses and by ensuring these eGovernment systems meet their users' needs, as well as increasing administrative transparency and accountability wherever possible.

- *Implementing high impact key services*. Public administrations should create a variety of eGovernment services with a strong and visible impact in meeting social and economic needs, including major projects delivering Pan-European benefits citizens and businesses. A fair and transparent market, including electronic procurement processes should be established to enable a range of companies to help administrations achieve this goal.

[12] These goals draw on: 1) European Commission (2006), i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, 2006, available at, http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/egov_action_plan_en.pdf and the EU Ministerial Declaration, Transforming Public Services (2005, 24 November), available at, http://www.egov2005conference.gov.uk/documents/proceedings/pdf/051124declaration.pdf

[13] This goal is also supported by an i2010 agenda for ICT inclusion.

- *Strengthening participation and democratic decision making*. The use of effectively designed and managed ICT-enabled communication, interaction and knowledge building should enhance citizens' engagement in democratic processes that affect outcomes in diverse social, cultural and economic activities at all levels in the EU.

- *Putting key enablers in place*. Appropriate technical, standards and other operational support is required to facilitate progress in eGovernment in the EU, for instance to promote smooth interoperability between eGovernment systems (e.g. in the use of eSignatures and for other aspects of electronic identification management).

The Project's Approach to Investigating eGovernment Barriers

The project has a broad and diverse scope in terms of issues covered and the spectrum of different national, regional, cultural and other contexts that can affect outcomes of relevant initiatives. Its investigations therefore include a variety of relevant approaches to identifying, evaluating and addressing barriers to eGovernment. Part 3 discusses the main methods followed:

- Extensive reviews and analyses by the project's partners of the factors that can block or facilitate attempts to develop and use eGovernment services to meet social, economic and political aims. This includes detailed analyses of the legal foundations on which eGovernment systems are built.

- An online survey by the Oxford Internet Institute (OII) to explore perceptions of the main barriers and their relative importance to key stakeholders.

- Case study research providing in-depth investigations within significant contexts in which eGovernment services have been developed and used to try to achieve vital aspects of the above EU eGovernment goals. The five case studies are: Digital Citizen Rights, eConsultation, Employment Mobility, Public Registries and Cross Border Public Tenders. These have been chosen to encompass activities across a representative range of eGovernment activities that affect Pan-European services as well as ones concerning a single jurisdiction at Member State, regional or local level.

- Consultation with key stakeholders to draw on their knowledge and expertise as eGovernment policy makers, users, recipients of services and developers of related systems. This involves a variety of activities, such as workshops, meetings, the establishment of an expert group and maintenance of an active website.

- A set of research questions to guide our investigations of eGovernment barriers and their minimization and avoidance. These are open-ended enough to tease out new developments, but have an emphasis on identifying and exploring key practical barriers experienced by stakeholders.

More details about specific methods used are provided in Part 3.

Seven Key eGovernment Barriers: An Initial Categorization

The first phase of our investigations has involved important investigations such as the reviews of existing eGovernment research, development of legal foundation analyses and the online survey. These have identified seven main categories of barriers that can block or constrain progress on eGovernment:

- 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. Inappropriate cost/benefit analyses can fail to release the flow of investment at the levels necessary to support future eGovernment innovation.

- Digital divides. Inequalities in skills, access to appropriate systems, knowledge and motivational support can limit and fragment take-up of eGovernment.

- 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 wide 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 and their facilitation of more sharing of information and service provision.

- Lack of trust. Heightened fears about inadequate security and privacy safeguards in electronic networks can undermine confidence in applications of eGovernment that might pose risks, such as through unwarranted access to sensitive personal information or vulnerability to online fraud or identity theft.

- 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.

These seven categories represent the visible peaks to which are tied a multitude of more specific barriers that are relevant at different governance, institutional and jurisdictional levels. That is why we have chosen the project's case studies to include specific examples at a number of such levels.

Studies of these and other possible key barrier categories will continue throughout the course of this project. For example, although early analysis of results from the OII online survey broadly support our initial barrier categorization, we are currently

undertaking more detailed investigations to determine the precise implications of this for the detailed definitions of the seven categories,

The Main Legal Dimensions of eGovernment Barriers

Within our overall aim of examining barriers to eGovernment, a key project focus is on relevant legal dimensions to our main barrier categories. This highlights how laws and regulations are core foundations for building policies affecting eGovernment within and between European, Member State and regional levels. For example, EC Directives relating to eGovernment include: Directives 1999/93/EC on electronic signatures; 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society; and 2002/58/EC on privacy and electronic communications). Detailed analyses of eight key legal dimensions provided in Part 4:

- Administrative law. This relates to the approach adopted in European states other than those based on the common law 'Anglo-Saxon' legal model. Administrative Law recognizes certain formal guarantees for citizens in areas where public bodies have significant power, and therefore shape outcomes from the deployment of eGovernment services. However, it does not address relationships between individuals. This could lead to a lack of legal security if legal adaptations to accommodate eGovernment are limited to the general regulation of private individuals, and thus do not affect Administrative Law. (See paper on this issue by Valero Torrijos in Part 4).

- Authentication and identification. These are elements of 'identity management', a crucial eGovernment concept that arises when the provider of an online service (e.g. a government department) needs to check the identity of an online user. Authentication involves establishing or confirming whether a person or other entity, such as a business, is authentic; identification establishes or confirms the identity of a person. These processes can become barriers if they are too cumbersome, costly or insecure. (See paper on this issue by Cuijpers and Nouwt in Part 4).

- Intellectual Property Rights (IPR). IPR and copyright laws that protect creative works can apply to many electronic services provided by governments, and in interactions between government and businesses and citizens. This can affect the exchange of eDocuments and digital multimedia (e.g. video) or the protection of data bases, software and other eServices and eProducts. Directive 2001/29/EC notes that: "copyrights and related rights protect and stimulate the development and marketing of new products and services and the creation and exploitation of their creative content". However, these rights could also be used to constrain (e.g. through charges that exacerbate digital divides) or block the sharing of certain digital contents. (See paper on this issue by Cuijpers and Nouwt in Part 4).

- Liability. In two-way and interactive electronic relationships between government, businesses and citizens, there is a need for a considered division of responsibility regarding damages resulting from a malfunction in the process or from inaccuracies in the information involved. Liability law seeks to achieve this, typically on the basis of general tort law and contracts governed by general contract law. The special role of government in society

requires particular consideration in addressing liability in relation to eGovernment. (See paper on this issue by Cuijpers and Nouwt in Part 4).

- Privacy and data protection. Rights relating to privacy and the protection of personal data are now included in a wide range of legislation at European and Member State levels, as well as in wider frameworks such as the European Convention on Human Rights. As these issues are at the heart of many types of eGovernment development, systematic and detailed consideration must be given to addressing them in ways that do not impair the achievement of eGovernment goals. (See paper on this issue by Dos Santos and de Terwangne in Part 4).

- Public administration transparency. The wide availability of public sector information and the openness of democratic processes (e.g. eConsultations, online forums) are key elements in promoting public administration transparency to help build trust in government in general, and eGovernment in particular. Freedom of Information (FOI) legislation is a key mechanism for giving the public more access to government information. However, differences between FOI Acts at national or regional levels have created some significant divergences between Member States – but harmonization has so far applied only to a limited number of areas. (See paper on this issue by de Terwangne in Part 4).

- Relationships between public administrations, citizens and other ICT actors. Laws and regulation can play an important role in promoting effective communication between citizens, business and government. For example, a general right to use online services in all their relationships with a public administration could increase confidence in eGovernment among citizens. And relationships between public administrations and the ICT companies able to provide the technical and financial resources required to help develop appropriate systems need to ensure the public interest is clearly protected. (See paper on this issue by Valero Torrijos in Part 4).

- Re-use of public sector information. Computerized public databases spread over different public services are being used for an ever increasing range of information, including data about citizens, business enterprises, land use, vehicles, health and most other areas of society. As exchanges between databases become more technically possible, issues of re-using data in different contexts are growing in significance, as recognized in EU Directive 2003/98/EC on the re-use of public sector information. (See paper on this issue by de Terwangne in Part 4).

Prioritizing Barriers and their Legal Dimensions

Table 1 presents tentative early findings illustrating a simplified rating of the significance of the main legal dimensions to the seven barrier categories we have highlighted. It is provided to help stimulate discussion and obtain feedback. We believe its offers some valid broad indicators, but should not be taken as precise and definitive evaluations of what are complex and highly subjective assessments. It suggests that all barriers have a number of significant or very significant legal dimensions, which indicates that there are no ‘single-bullet’ solutions that can

eliminate the many obstacles to effective eGovernment across Europe. Instead, the barriers are multiple, interrelated and frequently resistant to change. Coordinated action from across the EU is therefore necessary to help avoid potential blockages or to minimize the impacts of those that do occur. This should be based on a systematic analysis and plan that seeks to understand specific contexts of eGovernment developments and use.

Table 1. Relationships Between Barriers and Legal Areas

Barriers: Legal area:	Leadership failures	Financial inhibitors	Digital Divides	Poor coordination	Workplace and organizational inflexibility	Lack of trust	Poor technical design
Administrative Law							
Authentication and Identification							
IPR							
Liability							
Privacy and Data Protection							
Public Administration Transparency							
Relationships							
Re-use of Public Sector Information							

Key:

Very significant	Red light
Significant	Amber light
Not significant	Green light

PART 2: MAIN EGOVERNMENT BARRIERS AND LEGAL ISSUES

What is an eGovernment barrier?

One of the project's first tasks was to clarify the definition of an eGovernment barrier that it will use in its investigations. We wanted this to be more precise than an everyday understanding of barrier as a physical obstruction that prevents or inhibits access to a location. Although the kinds of barriers to eGovernment we are investigating do not usually have such physical manifestations, we have found much value in an analogy between eGovernment barriers and blockages in water pipes. This is relevant as the Internet can be viewed as a network of electronic 'information pipes', where clearing a blockage to ensure the free flow of digital information and ePublic Services is as critical as removing physical pipe blockages that prevent the availability of ample supplies of water.

Systems driving the flow of water are equivalent in eGovernment to the pressure applied by political and public administration leadership as well as by service providers and the private eMarketplace supplying ePublic Services. On the demand side, the needs of consumers of the water or of citizens, business and other eGovernment users are also vital factors. In some cases, sufficient pressure can itself dislodge a blockage. In other instances, specific action needs to be taken to remove whatever is stopping the flow. Preferably, the proper implementation of appropriate plans should prevent blockages from occurring or minimize their impact when the do happen (e.g. by incorporating appropriate filters in a water system or in eGovernment by developing a legal framework that facilitates rather than restricts re-use of public sector information and appropriate access to personal data in shared networked eServices).

This analogy helps understanding of how barriers are an aspect of a larger integrated system, just as clearing a water pipe blockage is only one element in providing such as vital utility. This is reflected in our project's aim of examining the separate but interrelated legal and organizational issues that underpin barriers to eGovernment. The pipeline metaphor also helped us to clarify our categorization of barriers in a number of ways, for instance in highlighting the 'pinch points' where blockages are most likely to arise and where the damage to achieving desired eGovernment goals is most likely to be most acute. An important insight revealed by the water pipe analogy is that laws and regulations should be best viewed as 'requirements' for eGovernment services, in the same way that a pump is a requirement for a water distribution system.

Just as when a badly designed or otherwise inappropriate pipe blocks water flows, legislation that is inappropriate in particular contexts can create legal barriers, for example by data protection rules preventing access to personal information or Employment Law that constrains desirable e-enabled organizational and work restructuring. Nevertheless, data protection rules to prevent unauthorized access to personal information about citizens is an example of a core requirement for many eGovernment applications, such as doctor–patient communication. If they are designed and implemented in appropriate ways, such rules can therefore become an essential basis for gaining public trust in the eServices they underpin. However, costs, technical shortcomings or misunderstandings about their practical implications could still become eGovernment blockages. Similarly, a provision in an Employment

Law could be smoothly accommodated in an eGovernment innovation within a public administration that has cordial labour relations, but be a focus of workplace resistance to an eGovernment initiative in an organization with poorer human relations management.

In developing a working definition of an eGovernment barrier for use throughout the project, we identified a number of factors to be considered in investigating the blockages to eGovernment progress. For instance, we feel it is necessary to determine through empirical studies the degree to which perceptions of a potential barrier (e.g. IPR or data protection regulations) become manifest as real blockages. There are also differences between barriers to demand (e.g. lack of awareness of eGovernment benefits among citizens, business users and public administrators) and those inhibiting supply (e.g. encompassing public administrations and commercial ICT suppliers in public–private projects). In studying such aspects, we are taking into account the ways in which the convergence of various digital ICT applications and channels is undermining many traditional distinctions between supply and demand (e.g. where citizens can perform online many activities once handled by government employees).

These considerations have led us to define ‘eGovernment barriers’ as follows:

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

Overview of the Barrier Categories

A prime consideration in finalizing the initial list of key barriers summarized in Part 1 was obviously to ensure that they only highlight the most significant areas. In addition, we sought to ensure they identify a comprehensive range of set of pillars to which cross-cutting themes can be anchored, as there are many issues that embrace different categories. For instance, at one stage we considered ‘lack of appropriate skills’ as a category on its own, but further analysis revealed important distinctions between the skills differences arising from digital divides in the general public and issues around inadequate training and capacity building among the specialists who design, develop, manage and deliver public services. On the other hand, financial inhibitors may arise within many categories (e.g. addressing the needs of minority groups or improving trust by creating more secure systems) – but it is such a fundamental issue that it has been identified as one of the key categories.

These examples indicate some of the complexities and challenges involved in developing clear-cut barrier categories. Feedback from stakeholders to date, including the online survey (see Part 3) indicates that they provide good coverage of the main challenges to eGovernment. The next phases of the project, including further detailed analysis of the survey data and the completion of the case studies, will explore the resilience of these categories as an aid to identifying and understanding the key barriers themselves and the cross-cutting legal and institutional ties between them. As this research progresses, we will continuously

reassess our definitions of the main categories, refining current ones or adding new ones when appropriate. Feedback from readers of this report is welcomed to assist our team in this work.

The case studies will be especially important in fleshing out answers to our research questions. For example, in the cases studies on employment mobility, public registries and cross border public tenders we will investigate how the sharing of data across departments can encounter barriers across a number of categories. These could include: poor leadership in gaining commitment from different partners to that sharing; perceived high costs of moving data into compatible or integrated forms; difficulties for some sections of the community in using shared information to their benefit; lack of coordination between departments sharing information; inter-departmental battles over new responsibilities and work allocation in a more shared, networked governance model; and incompatibilities between legacy and newer ICT systems that could constrain severely the sharing of information and ePublic Services.

The following sections illustrate the kinds of issues in the key barrier categories we will further investigate as the project progresses.

Leadership failures

Advances towards wider eGovernment take-up can be limited by failures in political and management leadership[14], such as a lack of clear vision or failure to provide appropriate planning – including adequate resources – to avoid or minimize the impacts of blockages in electronic pipelines. Management of the development of ICT systems in the public sector has a generally poor track-record[15], and the need to do this well becomes even more significant in projects targeting high impacts across many stakeholders and boundaries. The logic behind the adoption in the EU of an eCommission[16] framework is, in part, to lead by example in providing improved, more cost-effective, transparent and secure eGovernment services. Such leadership requires an ability not only to manage complex ICT-based projects but to motivate and support sustained commitment to eGovernment within public administrations and the use of eGovernment services by citizens. This requires effective management in addressing differences in interests, perceptions and understanding among different stakeholders to ensure such conflicts do not become blockages to eGovernment.

[14] The importance of leadership is highlighted in a number of documents e.g. United Nations (2003), World Public Sector Report: E-government at the Crossroads, New York, United Nations, available at, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan012733.pdf; and OECD (2003), Challenges for E-government Development, 5th Global Forum on Reinventing Government, Mexico City, 5 November, available at, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan012241.pdf

[15] Dutton, W. (1999), Society on the Line, Oxford, Oxford University Press, Chapter 7; Margetts, H. (1999), Information Technology in Government: Britain and America, London, Routledge.

[16] For more details about the eCommission see http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/1474&format=HTML&aged=0&language#fn1#fn1

Examples of leadership failure include:

- Low prioritization of eGovernment in public policies and resource allocation.
- Cycles of attention and inattention that lead to patchy, stop–go progress on eGovernment.
- Failure to learn from good practice.
- Inadequate marketing to reach and motivate target audiences in the general public and business.

Financial inhibitors

The costs of developing, implementing and maintaining ICT systems often dominate eGovernment cost/benefit assessments because they can be more easily identified and often arise before the benefits become visible. When competing with other critical demands on public resources, difficulties in calculating substantive tangible benefits to offset clear, often apparently high, costs can lead to the financial tap to eGovernment being tightened or turned off, thereby severely hampering the speed and scope of eGovernment progress.

The tangible costs that most readily fit the metrics used in traditional cost/benefit analysis techniques include those related to investment in systems and equipment (e.g. ICT hardware, software licences, network infrastructures and special ICT centres) and people (e.g. the public administration and technical and consultancy staff needed to manage, design, develop, market, operate, support and enhance eGovernment systems). Although some benefits can be seen in clear measurable terms (e.g. staff numbers and reductions in cost overheads), many cannot be defined with confidence in a similar way as they are too qualitative, intangible or unpredictably set in the future (e.g. improved quality of service, new services, responsiveness to citizen needs or avoidance of costs that would have been incurred using non-digital channels).

Examples of financial inhibitors include:

- Difficulties in establishing a firm connection between ICT innovations and actual outcomes, including benefits.[17]
- Costs of providing multiple channels overshadowing benefits of inclusivity.
- Short-term costs more politically relevant than long-term benefits.
- Lack of flexibility in exploring funding innovations (e.g. involving the private sector).

[17] For example, the EU MODINIS eGovernment Economics Project (eGEP) acknowledged the 'impossibility' at present of aggregating all economic activities within the Public Sector in the same way that economic activities are aggregated on a market-value basis in the private sector. See eGEP Economic Draft Final Version, eGovernment Economics Project (eGEP) Economic Model for Third Workshop (Deliverable D.3.2), p. 12 http://217.59.60.50/eGEP/Static/E_Interim.asp?ST=0

Digital Divides

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. These divisions range from users at the ends of electronic 'pipelines' who may not know that there is a 'tap', where to find it or how to turn it on – to those with much expertise who are capable of interacting in sophisticated ways as providers as well as consumers of digital content. It is particularly difficult to develop networked services that meet such greatly varying user perceptions, knowledge and capacities.

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"[18]. As part of this focus, eGovernment developments must satisfy crucial 'ease of use' criteria common to all ICT-enabled services. In addition, the multilingual, multicultural nature of the EU and public service nature of eGovernment activities creates requirements that could cause problems in achieving inclusive and efficient eGovernment throughout Europe. The study therefore treats the term 'usability' as covering the full range of capacities, user–system interfaces, support and training needed to make effective use of eGovernment services. The overall aim is to meet a fundamental user need: to have access in a convenient and affordable form to relevant eGovernment services at the times and places where they would be of most value to the user.

Examples of digital divide barriers include:

- Skills gaps between different sectors of society.
- Substantial variation in experience with ICTs across users, leading to different levels of trust and confidence in eGovernment.
- Lack of affordable technological access to eGovernment systems for some social groups or geographical areas.
- Differences in take-up and use within the same household (e.g. between the older and younger members).[19]

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

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

[19] For example, see Dutton, W. H., di Gennaro, C. and Hargrave, A. M. (2005), The Internet in Britain: The Oxford Internet Study (OxIS), Oxford, Oxford Internet Institute, available at, http://www.oii.ox.ac.uk/research/oxis/oxis2005_report.pdf

governance channels at EU, Member State, regional and local levels[20]. For instance, the diversity arising from the cumulative historical development of Administrative Law in different member States can require many locally-specific solutions to support reforms promoted by the EC to stimulate wider eGovernment take-up.

Effective coordination across the EU is particularly important because responsibility for directing public administration activity is frequently fragmented and shared across multiple levels, although the legal mandate of the EC deals only with Member States. For instance, EU Directives can seek to introduce more harmonization but the diverse contexts affected mean that different interpretations and actions could create substantial and disruptive tensions between stakeholders, as well as in the ways in which services operate in different arenas. The distance between the EU and other stakeholders could also block effective European-wide eGovernment. eProcurement in cross border public tenders (one of our case studies) is one of the initial high impact Pan-European eGovernment services targeted by the EC[21,22].

Examples of poor coordination include:

- eGovernment-related Directives that are differently interpreted or implemented to different degrees in EU Member States (e.g. those on data protection and freedom of information).

- Lack of coordination between regional and local government institutions.

- Failure to agree eSignature security processes.

- Government departments failing to agree and implement common procedures and standards to provide shared networked eGovernment services.

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 system that support activities cutting across traditional administrative responsibilities. 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.[23] However, prevailing practices can be difficult to change as they are designed to support certain patterns of communication and information exchange, while discouraging others. eGovernment

[20] For example, the OECD (2003), e-Government Imperative, 2003, available at, http://Webdomino1.oecd.org/COMNET/PUM/egovproWeb.nsf/viewHtml/index/$FILE/E-Government%20Imperative%20Final().pdf

[21] This aim is supported by the 2004 eProcurement Action Plan agreed with Member States. See also European Commission (2006), i2010 eGovernment Action Plan and European Commission (2004), Legal Framework for eProcurement from Directives 2004/18/EC and 2004/17/EC to Assist Cross Border Solutions, COM(2004) 841.

[22] Also see IDA (2002), Transborder eProcurement Study. Public eProcurement: Initiatives and Experiences: Borders and Enablers. Available at, http://ec.europa.eu/idabc/servlets/Doc?id=22188

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

initiatives often blur these boundaries and require appropriate changes to take account the of the new methods of operating and managing public services.

For example, the ability to share resources between public services using a variety of online and traditional channels is essential to providing efficient networked governance processes. Anything preventing this sharing can therefore be a significant barrier to eGovernment (e.g. IPR or copyright protection that bars access to information for certain stakeholders or fears of increased liability risks if the sharing of networked resources makes it difficult to clearly assign responsibility for an error). In opening opportunities for new online services, eGovernment could also create a need to support multi-channel services because traditional offline print, telephone and other facilities are still required for certain stakeholders[24]. The provision of such multiple pathways could add significantly to the complexity and costs of providing some ePublic Services.

Examples of workplace and organizational inflexibility include:

- Employment laws inhibiting flexibility in changing working practices or the deployment of staff.
- Departmental 'turf wars' involving competition over who is responsible for what in a networked service.
- Inadequate skills training and capacity building for management and staff[25].
- Reluctance to change a service or working practice that has operated well in the past.

Lack of Trust

Issues of trust, and the lack of it, have always been a strong ingredient in shaping the structures and practices of governance. It is therefore not surprising that a concern about 'cyber trust' in eGovernment is a crucial element in the take-up and effectiveness of eGovernment services. At the heart of these concerns is a 'trust tension'[26] 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[27], eGovernment raises particular trust concerns as so many public services require the handling of highly sensitive personal information in digital forms[28].

Low levels of trust in ePublic Service can be a major impediment to their take-up. This can be also be affected by general trends in perceptions of trust in government,

[24] See, for example, the multi-channel delivery of eGovernment services study by IDABC. Available at, http://europa.eu.int/idabc/en/document/3118/5644
[25] See, for example, EIPA (2005), Organisational Changes, Skills and the Role of Leadership. Available at, http://ec.europa.eu/idabc/en/document/4527/254
[26] See 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.
[27] 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, available at, http://www.oii.ox.ac.uk/research/publications.cfm
[28] See Part 4, de Terwangne, C., 'Privacy and Data Protection and eGovernment'.

such as those caused by the attitude of a public administration to transparency[29] and openness issues. To help overcome trust concerns, mechanisms in which there is wide confidence need to be developed to protect citizens from the unauthorized electronic disclosure of personal information, including the transfer of such data between public bodies or between public and private organizations.

Examples of areas where lack of trust is significant include:

- The 'Big Brother' fear of unwarranted government intrusion into private lives and business operations through the growing use of networked or integrated digital databases.

- Insufficient priority to implementing and promoting effective eGovernment security.

- Intrinsic 'cybertrust tensions'[30], 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).

- Public administration anxieties over liability for online content.

Poor Technical Design

eGovernment systems and services frequently fail or perform poorly because of the inadequate design and implementation of technical capabilities. Incompatibilities in hardware, software or networking infrastructures within and between public agencies and 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[31].

One of the most powerful benefits of the Internet was its creation of a truly open system, with full end-to-end flows across the network enabling smooth and efficient interconnections between ICT systems, applications and users. Some eGovernment services (e.g. web-based information, online publication of documents and the completion of tax returns online) can make effective use of the Internet's openness. However, many eGovernment services are based on the evolution of earlier public administration systems and ICT network infrastructures, which can create technical incompatibilities between systems within one within one administration (e.g. between back-office and citizen-facing networked services) or between systems from different Member States and those at European levels. To promote better interoperability, the setting of standards through law and regulation should wherever possible be

[29] The European Commission has launched a European Transparency Initiative. See http://ec.europa.eu/commission_barroso/kallas/transparency_en.htm

[30] Dutton, W. H., Guerra, G. A., Zizzo, D. J. and Peltu, M. 2005. 'The Cybertrust Tension in E-government: Balancing Identity, Privacy, Security', Information Polity 10: 13-23.

[31] Technical interoperability involved in "knitting together IT systems and software, defining and using open interfaces, standards and protocols in order to build reliable, effective and efficient information systems" is a key issue for the success of Pan-European services. See Communication on Interoperability COM(2006) 45 Available at http://europa.eu.int/information_society/eeurope/2005/doc/all_about/egov_communication_en.pdf

'technology neutral', by not favouring any particular supplier or proprietary brand. This could help to empower users to make decisions on system adoption and use, as well as reducing costs and enhancing general eGovernment interoperability.

Examples of problems caused by poor interoperability and usability design include:

- Online public services that are difficult to access and use[32,33].
- Incompatibilities between newer eGovernment systems and older 'legacy' systems (based on paper media or older computers).
- Failure to agree and implement global standards (e.g. eSignature identification).
- Inability to employ eGovernment services using devices (e.g. mobile phones or old personal computers) most easily accessible by particular users.

The Main Legal Issues Affecting eGovernment Outcomes

The following sections provide a short overview of each of legal issues explored in depth in Part 4.

Administrative Law[34]

Although initiatives promoted by EU Member States to develop the use of ICT in the public sector have generally sought to adapt their legal frameworks to meet the new public administration challenges, some essential Administrative Law reforms are still necessary to address barriers imposed by certain regulations within this legal model. For instance, when 'traditional' Administrative Law rules are not adapted sufficiently to specific requirements regarding ICT capabilities, a serious obstacle to the implementation of electronic public services may be created.

The potentially most significant barrier category relating to Administrative Law is in workplace and organizational flexibility, as one of the most important challenges to introducing ICT in this field is to apply the technology as effectively as possible in operational contexts. Opportunities for productive eGovernment innovations could be blocked if insufficient attention is paid to adapting Administrative Law when moving from traditional procedures using paper-based documents to those undertaken using electronic media. Such adaptations could also require a high investment in the electronic media employed, which could become a financial inhibitor. Strong leadership in prioritizing relevant Administrative law dimensions in the transition to eGovernment services is therefore important.

Administrative Law usually requires effective coordination among all public administrations concerned. In addition, trust can be significantly affected by an

[32] Such usability issues have been identified as key barriers among the general public (e.g. see Your Voice on eGovernment 2010 Online Public Consultation, October–December 2005, Report, January 2006, available at, http://europa.eu.int/idabc/servlets/Doc?id=24086 and in the EU's eUSER research project http://www.euser-eu.org

[33] Further, an EC Communication on eAccessibility defined specifically the technical barriers and difficulties that people with disabilities and others experience when trying to participate on equal terms in the Information Society was published in 2005. See eAccessibility, 2005, COM (2005) 425 available at, http://ec.europa.eu/information_society/policy/accessibility/com_ea_2005/a_documents/com_2005-0425-f_en_acte.pdf

[34] See Part 4, Valero Torrijos, J., 'Administrative Law and eGovernment'.

inadequate adaptation of traditional regulations relating to personal and direct contact between citizens, businesses and public bodies. For instance, if too low a level of guarantee is offered to private individuals and companies in these relationships, they may lose trust as users of eGovernment services because they seem to offer too low a degree of legal security (e.g. if decisions are automated).

Authentication and identification[35]

When moving to the use of ICT for government-related transactions, an electronic equivalent is needed to a signature, as used in paper-based systems to verify receipt of a welfare payment or to sign a cheque. This process should ensure: the authenticity of each party involved; the integrity of the contents of the communication; and the provision of confirmation about the communication if there is a dispute. Meeting these obligations can be technically complex (e.g. often relying on a third party 'certification authority' to guarantee the process, when the impartiality and trustworthiness of the third party also becomes an important issue). EU Directive 1999/93/EC sets standards on devices used to create eSignatures that also need to be considered.

Lack of coordination is a key potential barrier in authentication and identification activities (e.g. Directive 1999/93/EC seeks to harmonize a framework for the use of eSignatures in the EU but significant differences remain in relevant Member State legal rules). The significance of trust in any online transaction is highlighted by the way identity theft, fraud and error were among the main barriers that had to be addressed in eCommerce before commercial online services were able to grow. This is equally important in eGovernment.

Poor interoperability between eGovernment systems because of a lack of standardization in electronic identification and authentication technologies could be a major blockage to many eGovernment applications. The ICT expertise and facilities required to develop, implement and operate a secure feature like eSignatures can also be rather expensive and therefore act as a financial inhibitor. To avoid digital divides leading to the exclusion of certain groups from engaging in some eGovernment transactions, authentication and identification processes should be easy to use and reasonably priced, or free in some contexts. When authentication and identification processes are introduced in an organization, care should be taken in understanding and addressing the reasons why some management and staff could resist such innovations, perhaps in ways legitimized by laws (e.g. if security checks involve the processing of personal data from employees).

Strong leadership is therefore important to address these potential barriers, in order to avoid the slow or troubled introduction of authentication and identification processes whose satisfactory implementation could facilitate wider eGovernment take-up.

[35] See Part 4, Cuijpers, C. and Nouwt, J., 'Authentication and Identification in eGovernment'

Intellectual Property Rights[36]

The implications of IPR issues on specific forms of eGovernment communication and service delivery are of great importance for public administrations in terms of protecting its own rights and in avoiding liability for a breach of IPR when disseminating the creations of others (e.g. when publications are made by private parties on the order of a public authority). There are numerous types of electronic content that could be subject to IPR, copyright, patent and similar legal protection mechanisms (e.g. architectural drawings in planning department archives; databases; software; or patents on technological components in an electronic network). In general, if such rights and protection are too strong, then they could seriously impair the development and use of ePublic Services; but if they are too weak, the lack of security for content providers could equally significantly lead to barriers to the availability of key information and services that could be of much benefit to citizens and businesses.

Management leadership is therefore important to ensure attention is given to maintaining and appropriate balance in meeting IPR requirements. These have financial consequences that could become a serious barrier to eGovernment, for instance in relation to costs of accessing protected information and for software licences. The ways such costs could lead to the exclusion from certain services of citizens on the disadvantaged sides of certain digital divides has been a stimulus to explorations of the use of free and open source software[37].

Coordination and harmonization are important issues along this legal barrier dimension as there are various provisions relating to IPR, copyright and related issues in EC Directives such as 2001/29/EC on copyright harmonization, 96/9/EC on databases and 2003/98/EC on the re-use of public sector information. IPR controls could restrict sharing information in flexible ways, which could affect the need to support new forms of workplaces and organizational processes and structures in order to make optimum use of ICT-enabled networking capabilities.

A lack of trust in eGovernment could be addressed successfully through the development and monitoring of effective legal IPR requirements, both for those creating and supplying the content of eGovernment information services and for users relying on the quality and legality on the services they receive. However, copyright protection on proprietary software can lead to significant interoperability problems, which has been another impetus to examining the wider use of open source software licences that are less restrictive that those for copyrighted proprietary software products.

Liability[38]

There may be a higher risk of a malfunction leading to greater damages in electronic communication than when using non-electronic channels. It might also be harder to ascertain and prove where responsibility for an electronic malfunction lies, or to trace a malignant third party interfering with an eGovernment process. Different legal

[36] See Part 4, Cuijpers, C. and Nouwt, J. 'IPR and eGovernment'
[37] See, for example, the MODINIS initiative on Free/Libre/Open Source Software (http://www.flossworld.org).
[38] See Part 4, Cuijpers, C. and J. Nouwt, J., 'Liability and eGovernment'.

approaches within the EU regarding contractual and non-contractual liability can become a particularly serious barrier in eGovernment because the circle of parties involved frequently is generally much larger than those engaged in a non-electronic communication. The aggregation and integration of information into electronic databases can also lead to severe privacy and data protection liability risks. And Pan-European services might increase liability fears if complicated technical infrastructures and a lack of legal uniformity make liability assessment difficult.

All these circumstances could inhibit moves to change from non-electronic to electronic means of communication and service delivery, as well as to the development of new electronic services. On the other hand, appropriately designed ICT capabilities can help to detect and prevent inaccuracies and other causes of liability actions.

Financial inhibitors and lack of trust are likely to be the barrier categories most closely related with liability. The introduction of eGovernment innovations can lead to substantial financial provisions being factored into cost/benefit analyses of these developments, as well as concerns being raised about the degree to which an individual or unit might face new, difficult-to-anticipate liability risks.

Poor coordination in relation to legislation is tightly connected to liability, both in terms of broad aspects (e.g. differences in related legal provisions across the EU) and in liability assessment within an organization (e.g. when difficulties in identifying responsibility for liability arise when many stakeholders share networked resources). Coordination can be improved if there is close cooperation between experts from different scientific disciplines and relevant government actors. Interpretations of the impact of potential liability damages in cost/benefit analysis can also be closely related to workplace and organizational inflexibility.

Given the range of potential barriers arising from liability, including possible substantial legal penalties, leadership in addressing this legal dimensions is again clearly important.

Privacy and Data Protection[39]

Privacy and data protection legislation, regulation and guidance are relevant to all of our seven barrier categories because they are fundamental to most ePublic Services (e.g. those requiring access to public documents containing personal data and the sharing and re-use of public sector information). Rules protecting personal data can become barriers if they prevent or constrain some activities, such as in the processing of information about individuals or the transfer of data between public bodies and other entities. This could hinder, for example, the development of businesses offering information services or information products incorporating personal data if data protection obligations become, or appear to become, too burdensome on the controller of the collection and use of that information.

Coordination is one of the most potentially significant legal blockages along this legal dimension. For instance, clear guidance is needed to assist in assigning

[39] See Part 4, de Terwangne, C., 'Privacy and Data Protection in eGovernment'.

responsibility when data is mishandled or errors are created in shared networked services. At an EU level, improved coordination is vital because legislative approaches and solutions developed by various Data Protection Authorities are sometimes very different or even conflicting, which can create significant blockages to the development and use of some eGovernment systems. A number of initiatives have been established at a European level, such as the European Data Protection Supervisor, to help improve such coordination.

Despite these potential problems, the protection of personal data could be compatible with the development of eGovernment applications, provided an appropriate balance is maintained between a public administration's requirement to improve the efficiency and quality of its services and the need to protect individuals' personal details from unwarranted intrusion.

Public Administration Transparency[40]

As Freedom of Information Acts are the key legal vehicle for promoting public administration transparency through eGovernment, an important indication of the barriers to such transparency is highlighted by the exceptions to transparency contained in different FOI Acts. These exceptions vary greatly according to the different legal, historical, political traditions in Member States. A frequent lack of public awareness of the availability of a vast range of information, difficulties in locating information, inadequate access to appropriate technological tools or 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. Traditional FOI Acts are also mainly focused on transparency provisions that are 'passive' (requested by a citizen) as opposed to 'active' (spontaneously made available by government), although there is a trend towards promoting a more active approach.

One of the barrier categories most relevant to this area is the digital divides represented by the way knowledge and skills are distributed among users who wish to gain access to electronic networks, for example in the extent to which easy-to-understand 'meta-data' guides are provided to help find what information is available. In certain countries, fees perceived as being too high are charged for access, thereby discouraging requests for information. Language can be an important barrier, even when transparency is legally guaranteed in a Member State.

At the EU level, there is general lack of coordination with regard to access to public sector information, except for that on the environment. Structural barriers add to the coordination difficulty (e.g. the federal structures of some States that accentuate the disparity of access policies), as well as significant differences between Member States or regional levels (e.g. in provisions for active transparency and restrictions on access). Transparency is now generally seen to be a fundamental condition for public trust in government activities, including eGovernment services. 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.

[40] See Part 4, de Terwangne, C, 'Public Administration Transparency and eGovernment'.

Relationships between Public Administrations, Citizens and other ICT Actors[41]

Without a general right to use online services in all their relationships with a public administration, citizens may lose confidence in eGovernment. This could hinder the demand for, and establishment, of new eGovernment services (e.g. when an ePublic Service allows only for a narrow range of applications that have been previously and expressly sanctioned by the administration concerned – but which may not be those citizens and businesses consider to of most value to them). In relationships between public administrations and ICT companies, it is important to avoid any bias toward a particular firm or technology that could be contrary to the rules on free competition guaranteed at a European level and by Member States' regulations on public contracts.

Poor coordination and inadequate technical design are the two main barrier categories affecting this legal dimension. Coordination is one of the most essential factors in implementing networked electronic public services and in the more general exchange of information between public administrations and other stakeholders. Effective coordination is a critical requirement in the provision of high quality public services when a public organization decides it should be based on a decentralized model that best supports a networked eGovernment model. Technical incompatibilities and poor design can also become substantial operational blocks to effective relationships between public administrations, citizens and other actors, even within a framework that could otherwise supports effective relationships.

The focus on supporting relevant needs of citizens and companies that can be brought by strong leadership can obviously assist in developing eGovernment relationships. The most notable financial inhibitor could be the potentially high cost of implementing multiple channel systems to support a wider range of relationships between multiple stakeholders. Digital divides can also be affected when eGovernment services are designed mainly to solve internal administrative problems rather than focusing on the needs of other stakeholders. Prioritizing a wider perspective than that which focuses on an internal government perspective can assist to meet eGovernment challenges requiring much workplace and organizational flexibility to resolve. The absence of a wide recognition of citizens' right to contact public administrations through electronic means may cause a lack of trust in eGovernment services, specially when citizens and businesses compare ePublic Services with eCommerce offered by private companies.

Re-use of Public Sector Information[42]

Directive 2003/98/EC on the re-use of public sector information (PSI) 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 the initial purpose related to the public task for which the documents were produced. This 'PSI Directive' is important because many eGovernment services depend on such re-use, but 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

[41] See Part 4, Valero Torrijos, J., 'Relationships between Administrations, Citizens and Other ICT Actors'.
[42] See Part 4, de Terwangne, C. 'Re-Use of Public Sector Information in eGovernment'.

circumstances. As PSI re-use system also depend on the access regimes of the Member States, their implementation varies between Member States as well as sometimes between different governance levels within a nation.

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 has an imprecise reference to ‘a reasonable return of investment’ when fixing charges for the re-use of public documents, which 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 potential legal barrier.

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 elucidations on the principle of whether re-use itself should be allowed. The lack of a PSI re-use culture in most Member States can lead to blockages in workplace and organizational processes and structures when they need to be adapting to take account of eGovernment initiatives. For example, in the relatively underdeveloped market of environmental information, obstacles are often caused by public administrations who are not accustomed to locating appropriate information or negotiating with the private sector. Some public sector documents are excluded from the scope of the PSI Directive, such as those for which third parties hold the IPR. More generally, the Directive has not solved the problem of divergences of national legal regimes regarding IPR or data protection. 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.

PART 3: THE PROJECT'S RESEARCH METHODS

Investigations of the diverse matrix of dimensions relevant to eGovernment barriers in the EU have followed four main routes, backed by a set of guiding questions. These methods are outlined in this part.

Extensive Reviews and Analyses by the Project's Partners

Drawing on the extensive specialist knowledge among the project's partners in the project's initial phase has enabled us to review critically a wide collection of existing work on eGovernment to assist in the identification and analysis of the key obstacles to eGovernment and in their main legal dimensions. This has examined outputs from a number of EU research programmes, including IST[43] (e.g. QUALEG, SMARTGOV, EFORUM, EUSER KEELAN, GUIDE, PISA); IDABC[44]; eTEN[45] (e.g. CLAIM, PEELS, SUPER, RISER, SETS); eEurope2005[46]; i2010[47]; SIMAP[48]; eContentplus[49]; and the Safer Internet Programme[50]. Other sources include: legal doctrine; case law; case studies; research by NGOs (e.g. UNESCO[51], UNPAN[52]) and by companies (e.g. Accenture[53] and the Economist Intelligence Unit[54]); and legislation at national, supranational and international levels. In examining the vital legal foundations underlying eGovernment developments, detailed papers have also been prepared by specialists in different legal fields (see Part 4).

These reviews and analyses have infused our identification and exploration of key eGovernment barriers, and we continue such reviews and analyses as part of the ongoing process of updating of the team's knowledge base on relevant issues.

The Online Survey

An online survey carried out between May and June 2006 by the OII aimed to provide a detailed picture of the perceived barriers to eGovernment in the EU, including how these perceptions might vary across stakeholders and between the regions and nations of the EU. It was completed by almost 1000 key public administration, business and expert stakeholders who are engaged in eGovernment activities at local, regional, national or Pan-European levels. The survey was available in four languages (English, German, French and Spanish) and was advertised widely via numerous eGovernment lists, websites and personal contacts. The results will complement previous online and offline surveys examining barriers to

[43] http://europa.eu.int/information_society/activities/egovernment_research/projects/egovernment_projects/index_en.htm
[44] http://europa.eu.int/idabc
[45] http://europa.eu.int/information_society/activities/eten/library/about/themes/egovernment/index_en.htm
[46] http://europa.eu.int/information_society/eeurope/2005/index_en.htm
[47] http://europa.eu.int/information_society/eeurope/i2010/index_en.htm
[48] http://simap.eu.int/
[49] http://europa.eu.int/information_society/activities/econtentplus/index_en.htm
[50] http://europa.eu.int/information_society/activities/sip/index_en.htm
[51] http://portal.unesco.org/en/ev.php-URL_ID=29008&URL_DO=DO_TOPIC&URL_SECTION=201.html
[52] http://www.unpan.org/egovernment.asp
[53] http://www.accenture.com/
[54] http://www.eiu.com/

eGovernment and related areas, such as: the eUSER[55] study that explores online public services in the domains of eGovernment, eHealth and eLearning with a focus on the perspectives and needs of the user; the UNDERSTAND[56] project that investigates eGovernment at the regional level across Europe; a Pan-European Survey of Administrations Officials[57]; and a study of eGovernance by UNESCO[58].

Our survey questionnaire asked participants to rate the relative severity of 30 barriers to eGovernment. It also solicited other personal information (e.g. ICT skills, eGovernment experience, date of birth and country of residence) that could assist analyses of the results. Survey responses are currently being fully analysed and the detailed findings will be used to complement and inform other methods used in this project to refine our understandings of key barrier categories and their main legal and organizational dimensions. A final report will be available in autumn 2006, when it will be published on the project's website.

From the analysis of the survey results to date, the top five most significant blockages to eGovernment appear to be:

- coordination across central, regional and local levels of government [poor coordination barrier category];
- resistance to change by government officials [workplace and organizational inflexibility];
- lack of interoperability between IT systems [poor technical design];
- low levels of Internet use among certain groups [digital divides]; and
- lack of political support for eGovernment [leadership failure].

Perceptions of barriers are also significantly related to experience factors, such as ICT skills and country of residence.

Case Study Research

We recently started investigations into carefully selected case studies, which are beginning to provide more in-depth understandings of practical examples of barriers to eGovernment and their wider implications. A total of five cases will be examined during the course of the project. These are broadly defined to enable the project team to study eGovernment across Europe, drilling down into specific examples embedded at local, regional, national and/or Pan-European levels in sufficient detail to assess critically the legal–institutional dynamics of their success or failure. The completion of these case studies will give the project team more informed insights into the kinds of interventions that could facilitate eGovernment at levels in the EU.

[55] http://www.euser-eu.org/Default.asp?MenuID=8
[56] UNDERSTAND (2005): Results Synopsis, available at, http://www.understand-eu.net/
[57] Heinderyckx, F. (2002), Assessing eGovernment Implementation Processes: A Pan-European Survey of Administrations Officials, in Traunmuller, R. and Lenk (Eds). EGOV2002, LMCS, pp 111-115.
[58] UNESCO (2002), Country Profiles of e-Governance. Available at http://portal.unesco.org/ci/en/ev.php-URL_ID=5305&URL_DO=DO_TOPIC&URL_SECTION=201.html

The initial case studies are: Digital Citizen Rights; eConsultation; Employment Mobility; Public Registries; and Cross Border Public Tenders. A brief summary of each is provided below. Work has begun on eConsultation and Digital Citizen Rights cases and the remaining three will begin in autumn 2006. Such work will complement existing benchmarking data[59] and other information on eGovernment in the 25 member states[60], as well as contributing to building up a database of good practice in this area[61].

Digital Citizen Rights

The key emerging issue of Digital Citizen Rights introduces important new questions of equity and justice to the provision of online public services, participatory eDemocracy initiatives and the general movement of government administration to online channels. This case study will be conducted in two phases.

First, a multi-country analysis will analyse quantitative data to obtain an overview of what is happening in this area. Examples include cross-national figures on Internet penetration (e.g. via the OII's involvement in the World Internet Project[62]) and cross-national figures on availability and take-up of eGovernment services produced at Member State level and by the EU, NGOs like the OECD and private market research companies[63]. The variables to be examined will include: level of Internet penetration; degree of eGovernment activity (in terms of availability and use); level of Digital Citizen Rights (e.g. relating to accessing, transmitting and storing information); GDP per capita; degree of country decentralization; size of government; and length of democratic governance.

The second phase will be based primarily on qualitative research. In-depth studies will be made of two or three countries with similarities across all control variables but distinct differences in levels of eGovernment and Digital Citizen Rights measures. For each selected country, the quantitative measures explored in the first phase will be complemented by a more qualitative analysis of relevant initiatives in each country. Interviews will also be undertaken with key stakeholders (both users and producers) that emerge from the research.

eConsultation

eDemocracy is an important eGovernment application in the EU (e.g. to strengthen participation and democratic decision making in Europe, which is an objective of the i2010 eGovernment Action Plan). For instance, ICTs provide a means for extending citizens' access to public information and decision-making that opens up many new

[59] For example, European Commission (2004) Online Availability of Public Services: How is Europe Progressing? Web based Survey on Electronic Public Services - Report of the Fifth Measurement. Available at, http://europa.eu.int/information_society/soccul/egov/egov_benchmarking_2005.pdf

[60] For example, data from Eurostat (http://epp.eurostat.cec.eu.int/portal/page?_pageid=1090,30070682,1090_33076576&_dad=portal&_schema=PORTAL) and European Commission (2005) eGovernment in the Member States of the European Union. Available at, http://europa.eu.int/idabc/en/document/4370/254.

[61] http://www.egov-goodpractice.org/

[62] The World Internet Project covers over 20 countries (www.worldInternetproject.net), including the OII's Oxford Internet Surveys (OxIS) in Britain (www.oii.ox.ac.uk/research).

[63] For example, data from Eurostat and commercial companies, such as, Taylor, Nelson Sofres.

opportunities for changing who gets access to politicians and governments – as well as who politicians and governments can reach with their own messages. Decades of experiments with eDemocracy applications aimed at enhancing democratic participation in governmental processes have ranged from providing electronic voter guides, to supporting eVoting and online polling of citizens. These efforts are increasingly moving towards a focus on better informing and involving citizens in governmental decision-making and deliberation.[64] One of the most feasible and promising efforts over recent years to achieve this been through the promotion of electronic consultations.

Such eConsultations are particularly important to the Commission as an aid to developing some degree of psychological proximity between the Commission and citizens despite the EU's vast geographical distances.

This study will start by examining work on eConsultation across Europe (e.g. the European Parliaments Initiative (EPRI)[65] and DEMONET[66]). It will select a number of embedded cases from regional through to European Parliamentary level to examine aspects of good practice, analyse barriers to further activity and recommend guidance on policy implications. Examples of initiatives already identified include: eParticipate[67]; Madrid Participa[68]; Scottish Parliamentary Initiative[69]; and Toute l'Europe[70].

Employment Mobility

As European citizens can generally study, live and work in any of the 25 Member States, employment mobility is an important and interesting example of a high impact ePublic Service designed around citizens and business needs, as is highlighted in the i2010 eGovernment Action Plan.

In addition to the benefits for individual citizens, enabling the mobility of workers across Europe can also increase economic competitiveness by making the labour market more flexible and adaptable. The ways in which employment mobility is facilitated across Europe by ICT-enabled networks will be examined in this case. In its first phase, we will obtain a European-wide perspective on current initiatives in this topic at national and Pan-European levels. The second phase will undertake in-depth analyses of cases such as: national employment portals; EURES, the European Job Mobility Portal[71]; and commercial websites, such as StepStone[72] and EuroJobs[73]. Methods used for this will include interviews with stakeholders, usage analysis where available and document analysis. We will build on other work in this

[64] For an overview of issues of electronic democracy, see Dutton, W. (1999), Society on the Line, Oxford, Oxford University Press, pp. 173-93; and Coleman, S. and Norris, D. (2005), 'A New Agenda for e-Democracy', Forum Discussion Paper No. 4. Oxford: Oxford Internet Institute, University of Oxford, available at, http://www.oii.ox.ac.uk/resources/publications/FD4.pdf
[65] See http://www.epri.org/epriorg/EPRIorg_Home.php
[66] See http://www.demo-net.org/demo
[67] See http://www.eparticipate.org
[68] See http://www.madridparticipa.org
[69] See http://www.scottish.parliament.uk
[70] See http://www.info-europe.fr/debat
[71] Encompasses the European Economic Area, which consists of the 25 EU Member States plus Norway, Liechtenstein and Iceland (see http://ec.europa.eu.eures/index.jsp).
[72] http://www.stepstone.com/
[73] http://www.eurojobs.com/index.jsp

area, such as the EC-funded Mobility Case Study[74] examining the reduction of the 'administrative burden' of mobility. And we will collaborate with other current research projects of relevance (e.g. the recent MODINIS study, Innovative Adaptive Pan-European eGovernment Services for Citizens in 2010 and Beyond[75]).

By analysing the barriers to the use of eGovernment systems to facilitate employment mobility will be explored we hope to support further Pan-European initiatives being developed in this area, such as a European skills portal to complement EURES.

Public Registries

The numerous public registries for businesses and citizens within Europe present a number of interesting legal and organizational challenges. Such digital registries can lead to back-office efficiency gains as well as improved convenience and accessibility for citizens and businesses. However, a number of the organizational and legal issues discussed above need to be considered if these benefits are to be achieved (e.g. coordination, authentication and identification, public administration transparency, re-use of public sector information and Administrative Law). This case study will explore the barriers and the associated legal and institutional foundations involved with public registries in member states and at Pan European level.

We have identified a number of interesting cases and initiatives to explore at national and Pan-European levels. For example, Belgium has launched the Crossroads Bank for Enterprises, an integrated business register where each registered business is attributed a unique identification number that is linked to a set of information stored in a central database. This unique identifier is maintained centrally and used as primary key to exchange information between Belgian administrations. Such an initiative eliminates the need for businesses to provide the same information to several administrations, and makes possible the delivery of 'joined-up' services to enterprises.[76] Given the increasing importance of the European single market a number of projects are now explore a Pan-European focus. For instance, the European Commission has supported the RISER[77] service providing a trans-European eService on European Civil Registration, which enables online users to request official information from civil registries across borders.

This study will also be conducted in two phases: starting with an overview of activity across Europe, followed by a selection of the in-depth cases in a sample of European contexts.

Cross Border Public Tenders

eProcurement can increase the efficiency of government through the simplification of administration systems affecting the tendering process (e.g. saving time, increasing

[74] IDABC (2005) Mobility Case Study Final Report. Available at: http://ec.europa.eu/idabc/servlets/Doc?id=24484
[75] See http://ec.europa.eu/information_society/activities/egovernment_research/projects/i2010_studies/index_en.htm
[76] See European Commission (IDABC) (2005), European eGovernment in the Member States of the EU, available at, http://ec.europa.eu/idabc/servlets/Doc?id=21035
[77] The service has been realised by an international consortium from Germany, Poland, Hungary, Austria, Estonia and Ireland (http://www.riser.eu.com).

transparency and improving coordination).[78] Indeed, the i2010 eGovernment Action Plan estimated that electronic procurement and invoicing could result in annual savings of tens of billions of euros[79]. The recent Directives 2004/17/EC and 2004/18/EC[80] address issues related to procurement procedures, such as the rules on advertising and transparency of public procurement. However, there are still outstanding problems in this area (e.g. poor coordination, workplace and organizational inflexibility and poor technical design). These arise from the different interpretations of the Directive and the changes required for the efficient and effective widespread adoption of eProcurement.

An emerging challenge for cross border tendering arises when two or more Member States wish to launch a common tender. As this could lead to a number of benefits from economies of scale, the eGovernment Action Plan sets out plans covering 2006–2010 for cooperation between the Commission and Member States to investigate and develop cross border eProcurement solutions[81].

In our study in this area, we will explore the associated legal and organizational considerations by analysing current documents and following cases where such efforts are being made. The aim will be supporting such developments by identifying possible gaps in the current European framework.

Consultations with Experts and other Key Stakeholders

An important aspect of our research is the encouragement of interactions among a range of key eGovernment stakeholders in order to obtain informed feedback to help us achieve the project's aims. There are three main ways this is facilitated: via the project website; through workshops held every six months; and the formation of an expert group. These activities can ensure the project's work is targeted appropriately and has the most value to those most closely involved in seeking to break the barriers to eGovernment. A broader objective is to raise discussion and awareness of such barriers, as failures and difficulties are generally less often openly discussed than more successful cases.

The project website (http://www.egovbarriers.org) contains access to a number of valuable eGovernment resources relating to the project and more broadly. A key feature of the site is an online inventory that encourages feedback and interaction from eGovernment stakeholders. The online inventory provides brief summaries, including country examples, related to each of the seven categories of barriers to eGovernment and their key legal dimensions. These summaries are linked to a

[78] OECD (2003), The eGovernment Imperative, available at, http://Webdomino1.oecd.org/COMNET/PUM/egovproWeb.nsf/viewHtml/index/$FILE/EGovernment%20Imperative%20Final().pdf

[79] http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/egov_action_plan_en.pdf

[80] Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

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

discussion board where visitors to the website can comment on the text and add their own experiences, case studies or other relevant examples.

Workshops held every six months enable interested parties to find out more about the research and participants to interact with the project teams to assist their future work. Three highly interactive, discussion-based workshops have been held to date, two in Belgium and one in the UK. A workshop report from each event is published on the project website. Three further workshops will be held, with Belgium, Finland, Spain and Portugal among possible venues. See http://www.egovbarriers.org/?view=events for more details of past and future events.

An expert group has been set up consisting of about thirty specialists in eGovernment from a diverse range of backgrounds, including public administrations, business and research. Its role is to steer the project by providing:

- direction in helping to identify key barriers to eGovernment, together with practical illustrations of these barriers;
- input to the inventory of legal, regulatory and organizational barriers to eGovernment;
- identification of good practice in overcoming barriers, including suggestions for case studies;
- promoting the project within their own administration or organization and elsewhere; and
- commenting on the project's findings and drafts of its case studies and final report.

Research Questions to Explore and Build on the Barrier Categories

One of the earliest project tasks was to develop a set of questions that could be used to shape the project's surveys, case studies, expert discussions, focus groups and other engagements and research. These seek to elicit data and informed perspectives on specific problems experienced by representative key stakeholders. Legal and organizational issues are the prime focal points for these questions (e.g. relating to the provision of an EC Directive and related Member State laws or the workplace implications of a move to a more networked model of public administration). However, we also recognize the central significance of certain social, cultural and technical dimensions to eGovernment barriers.

The following are examples of the kinds of questions the research addresses in relation to each barrier category. The analyses by members of the project team of the legal foundations of these barriers in Part 4 offers further discussion of these questions and some initial answers. As the project progresses and the questions are refined and more answers obtained, we will formulate guidelines for policy and practice to help avoid or minimize the obstacles encountered in efforts seeking to achieve key eGovernment goals in the EU.

Lack of Leadership

- What evidence is there of the effects of any lack of political and management will behind eGovernment (e.g. a failure to motivate high-priority commitment to eGovernment initiatives; persistence of vertical barriers between departments; continuing conflicts between stakeholders disrupting progress towards eGovernment)?

- What are the main causes of the lack of adequate leadership (e.g. lack of technical expertise among top managers; insufficient incentives; a move to eGovernment perceived as hampering the achievement of other political, administrative or personal objectives, such as preserving government confidentiality, achieving budget reductions or disrupting career progression along traditional pathways)?

- What are the patterns of leadership in different phases of the initiation, design, development, implementation, marketing and sustained support and development of eGovernment services? Are there particular points of vulnerability in this lifecycle where leadership interest fades?

- To what extent are efforts being made to learn from good practice[82] and what are the key factors blocking such learning (e.g. too frequent moving of top public administration managers to new positions; use of external contractors who keep learning to their own enterprises)?

- Which eGovernment services are prioritized most by government and public administration leaders (e.g. in meeting eDemocracy and Freedom of Information transparency aims)? Which of these and are given insufficient – or too much – priority?

- What key factors make the difference between poor and effective leadership?

- Which sources of leadership other than from politicians and administrators have most impact (e.g. technical staff, business, the media, NGOs, civil society activists)?

Financial Inhibitors

- In what ways do traditional financial accounting methods block investment in high-risk, but potentially significant, eGovernment investments whose main payoffs (qualitative and quantitative) are most likely to be achieved in the longer term?

[82] The need to learn from good practice is an important issue (e.g. European Commission (2006), i2010 eGovernment Action Plan and European Commission (2003), The Role of eGovernment for Europe's Future, COM (2003) 567, available at, http://www.europa.eu.int/information_society/eeurope/2005/doc/all_about/egov_communication_en.pdf There are a number of EC mechanisms in place to share good practice, such as the Good Practice Framework (http://www.egov-goodpractice.org) and the eGovernment Observatory (http://ec.europa.eu/idabc/en/chapter/140). However, the lack of learning from the experiences of others is a continuing issue that impedes eGovernment development.

- What are appropriate metrics for assessing the benefits of eGovernment services? What kinds of further studies[83] could help to develop more appropriate impact assessments to promote innovation, while maintaining effective costs controls?

- What have been the most successful examples of innovative funding mechanism for eGovernment (e.g. through partnerships with business or tax incentives)?

- How far is the meeting of inclusivity goals hampered by perceived costs of the developments needed to fulfil that objective? How widely have existing 'accessibility' standards for the disabled (e.g. citizens with poor eyesight or dyslexia) been implemented, at what cost and with what benefits?

- To what extent have the costs of providing effective security and trust systems (e.g. using eSignatures) inhibited eGovernment investment by raising the overall entry point for affordable investments?

- How significant are the increased costs for governments of meeting laws and regulations relating to eGovernment (e.g. relating to freedom of information or data protection). Are such costs a significant eGovernment barrier?

- How are the costs of software licences affecting investment in eGovernment? Are these costs leading to a greater use of free open source software?

Digital Divides

- What are the main difficulties (e.g. hard-to-use interfaces; inadequate or high-cost technological access; lack of skills or motivation to use eGovernment services; lack of ePublic Services meeting the needs of certain groups (e.g. less wealthy citizens; disadvantaged minorities; small businesses)?

- How far, and in what ways, does a lack of equitable eGovernment-related capacity and skills building among all sectors of society hamper eGovernment take-up?

- Are demands for inclusion putting a brake on eGovernment services (e.g. by raising the costs of service development and implementation to meet accessibility requirements, such as for minority language speakers or the visually impaired)?

- Are there examples of IPR or copyright restrictions being a barrier to eGovernment services?

[83] For example, the eGEP study recommends the establishment of a working group to agree an operational definition of eGovernment expenditure and a study to agree critical issues about measuring eGovernment value (see eGovernment Economics Project (eGEP 2006), Expenditure Study, Draft Final Version, 1 March, p. 60 (http://217.59.60.50/eGEP/Static/E_Interim.asp?ST=0).

- Is the absence of a general digital citizen right to use electronic means to contact public administrations putting a brake on eGovernment services?[84]

Poor Coordination

- In what aspects are cross-national differences in legislation and regulation resulting in constraints on broader eGovernment take-up, even where there are EU-wide harmonization efforts (e.g. in relating to IPR and copyright[85], liability[86], FOI[87], data protection and privacy[88] and digital signatures[89])?.

- What are the effects of eGovernment on communication and interaction between key stakeholders (public administrations, citizens, business, etc.)? [90]

- Are different government legal-administrative traditions (e.g. the Administrative Law and Common Law models) more or less discouraging to the promotion of eGovernment?[91]

- Have provisions in Directives (e.g. relating to IPR or authentication and identification) become barriers for the competitiveness of the European economy, and how could such provisions be altered to remove the blockages?

- In what ways do the current structure of Employment Law in Member States block or facilitate the restructuring of the public sector labour market in making moves towards realizing the full benefits from high levels of ePublic Services delivery and use?

- What are the implications of relevant global agreements on eGovernment within the EU (e.g. WTO's TRIPS Trade-Related Aspects of Intellectual Property Rights agreement[92])?

Workplace and Organizational Inflexibility

- To what extent, and how, are government priorities shaped by emerging concepts of digital citizen rights[93] and to what extent do these rights to access to eGovernment services in appropriate forms constrain or facilitate the development of new networked governance models and processes?

- What have been the effects of different interpretations by Member States of provisions in FOI-related regulations and legislation[94] (e.g. variations in

[84] See Part 4, Valero Torrijos, J., 'Relationships between Administrations, Citizens and Other ICT Actors'.
[85] See Part 4, Cuijpers, C. and Nouwt, J. 'IPR and eGovernment'.
[86] See Part 4, Cuijpers, C. and J. Nouwt, J., 'Liability and eGovernment'.
[87] See Part 4, de Terwangne, C., 'Public Administration Transparency and eGovernment'
[88] See Part 4, de Terwangne, C., 'Privacy and Data Protection and eGovernment'.
[89] See Part 4, Cuijpers, C. and Nouwt, J. 'Authentication and Identification and eGovernment'.
[90] See Part 4, Valero Torrijos, J., 'Relationships between Administrations, Citizens and Other ICT Actors'.
[91] See Part 4, Valero Torrijos, J., 'Administrative Law and eGovernment'.
[92] See Part 4, Cuijpers, C. and Nouwt, J., 'IPR and eGovernment'.
[93] See Part 4, Valero Torrijos, J., 'Relationships between Administrations, Citizens and Other ICT Actors'.
[94] See Part 4, C. de Terwangne, 'Public Administration Transparency and eGovernment'.

exceptions in FOI Acts and in charging policies regarding requests for information)?

- What have been the impacts in the EU of Directives relating to liability issues[95] (e.g. provisions in Directive 1999/34/EC on product liability and the eSignature Directive 1999/93/EC)?

- Has the introduction of secure electronic signature creation devices[96] been hampered by a perceived or actual over-specification of security requirements?

- How do EU regulations block or encourage intermediaries or other third-party providers of eGovernment services[97] (e.g. the eCommerce Directive's provisions regarding liability of intermediary service providers)?

- In what ways is data protection legislation constraining or facilitating the development of shared eGovernment services (e.g. because of prohibitions on data sharing and re-use[98])?

- What has been the impact on eGovernment of Directive 2003/98/EC on the re-use of public sector information[99]?

Lack of Trust

- What have been the practical implications of the ways in which information in databases have (or have not) been protected[100] by national provisions based on the Database Directive.

- What are the implications of a lack of harmonization of data protection across Europe and how can relevant Directives be modified to make them more effective?[101]

- What obstacles have there been to wider use of eSignatures, in addition to any harmonization issues across Europe?

- How does fear of identity theft, fraud or error affect citizens' willingness to use eGovernment services?[102]

- To what extent is eGovernment increasing or diminishing public administration transparency in terms of citizens' access to information about government operations and decision-making?

[95] See Part 4, C. Cuijpers and J. Nouwt, 'Liability and eGovernment'.
[96] See Part 4, C. Cuijpers and J. Nouwt, 'Authentication and Identification and eGovernment'.
[97] See Part 4, Valero Torrijos, J., 'Relationships between Administrations, Citizens and Other ICT Actors'.
[98] See Part 4, de Terwangne, C. 'Re-Use of Public Sector Information in eGovernment'.
[99] See Part 4, de Terwangne, C. 'Re-Use of Public Sector Information in eGovernment'.
[100] See Part 4, Cuijpers, C. and Nouwt, J., 'IPR and eGovernment'.
[101] See Part 4, de Terwangne, C., 'Privacy and Data Protection in eGovernment'.
[102] See Part 4, Cuijpers, C. and Nouwt, J., 'Authentication and Identification in eGovernment'.

Poor Technical Design

- Does a lack of standardization or interoperability of electronic identification and authentication technologies[103] remain a barrier to public sector eCommerce applications?

- To what degree are policies relating to ICT procurement technologically-neutral, and how is this affecting eGovernment take-up?

- What specific problems are posed by legacy ICT systems in moving to eGovernment service involving more modern systems (e.g. in the interoperability of older and newer systems and equipment)?

- How well are technical open systems standards being specified and followed?

- How is the use of open source software affecting interoperability?[104]

[103] By 2010 European citizens and businesses should benefit from secure means of electronic identification that maximize user convenience while respecting data protection regulations to identify themselves within their own or any other member state. The current Action Plan notes that there will be a pragmatic approach to cross border identification and authentication ensuring differences in national approaches and solutions are respected but not allowing this diversity to cause barriers to eGovernment. The eSignatures Directive is to be followed up and consideration given to the need for regulatory measures for overcoming barriers to the single market. See also Part 4, Cuijpers, C. and Nouwt, J., 'Authentication and Identification in eGovernment'.

[104] e.g. see Part 4, Cuijpers, C. and Nouwt, J., 'IPR and eGovernment' and Välimäki, M. (2005) 'Software Interoperability and Intellectual Property Policy in Europe', European Review of Political Technologies, December 2005.

PART 4: LEGAL FOUNDATIONS

Background

This section provides detailed analyses by the project's partners of the main legal issues identified in Part 2 as being important dimensions of the seven key barrier categories highlighted in this report.

The papers have been written by:

- *Dr. C Cuijpers and Dr. J. Nouwt, Tilburg Institute for Law, Technology, and Society (TILT), University of Tilburg, Netherlands*: Authentication and Identification; Intellectual Property Rights; and Liability.

- *C. Dos Santos and Professor Cécile de Terwangne, CRID (Centre de Recherches Informatique et Droit), University of Namur, Belgium*: Privacy and Data Protection; Public Administration Transparency; and Re-use of Public Sector Information

- *Dr Julián Valero Torrijos, University of Murcia, Spain*: Administrative Law; Relationships between Public Administrations, Citizens and other ICT actors.

The different styles of the authors are reflected in the papers. In later versions of this document, each paper will be more integrated into the overall document format.

Administrative Law and eGovernment

Dr Julián Valero Torrijos, University of Murcia, Spain

1. Description of the area

In most European states – but not those, such as the UK, influenced by the legal Anglo-Saxon model of public administration that is ruled by common law – public administrations are governed by a specific regulation ('Administrative Law') that is different from those which govern the relationships between individuals. Such Administrative Law is characterized by the assignment of significant powers to public bodies and the recognition of relevant formal guarantees for citizens, based typically on a correct observance by public administrations of a legally predetermined sequence of steps. If the rules specified in Administrative Law are made too rigid to accommodate the changes made possible by the use of ICTs, they could become obstacles to the effective implementation of eGovernment and erode confidence in eGovernment among citizens. On the other hand, if legal adaptations to accommodate eGovernment are limited to the general regulation of private individuals and don't affect Administrative Law, the lack of legal security regarding the use of ICT in administrative activities could become a major barrier to the modernization of public administration.

2. Why could there be barriers to eGovernment in this area?

Generally, initiatives promoted by EU Member States to develop the use of ICT in the public sector have involved an intensive effort aimed at trying to overcome potential problems arising from the need to adapt the legal framework of their public administrations to the new challenges and problems. However, relevant essential reforms are still necessary in many cases in order to overcome some of the barriers imposed by the existence of specific Administrative Law regulation.

For instance, when 'traditional' Administrative Law rules are not adapted sufficiently to specific requirements related to ICT capabilities, a serious obstacle to the implementation of electronic public services may be created. Moreover, much new ICT-related legislation has been passed recently by Member States as a necessary adaptation to relevant European Directives, especially those related to digital signatures (Directive 1999/93/EC), eCommerce (Directive 2000/31/EC) and personal data protection (Directive 2002/58/EC). One of the main legal requirements in these fields is to fit modern regulation to the important requirement for a single, consolidated framework based on its own principles.

Therefore, an inadequate or non-existent adaptation of Administrative Law to the requirements of technology may involve a lower level of guarantee for private individuals and companies, which could threaten their essential role as users of electronic public services. This would pose a very serious problem since the validity of administrative acts and respect for the rights of citizens may be damaged and, therefore, the modernization process involving eGovernment could be made much more difficult.

3. What is the European context for this area, including legislation, policy statements and institutional arrangements relevant to this topic?

Many member States have not taken sufficient account of the existence of a specific legal frameworks for public administration when implementing reforms promoted by the EU in the field of ICT, such as the Directives on data protection, digital signature and eCommerce. One reason for this is the absence of a general competence reserved to the EU in this area. Another is the intensive influence in some states of the legal Anglo-Saxon model of public administration based on common law. As a consequence, the implementation of these Directives by many of the Member States belonging to the 'continental model' of public administration based on Administrative Law has created some national rules that are not sufficiently adapted to the specific requirements of public administration regulations. Underestimating the particular needs of public administration activities can be considered as a serious potential barrier to eGovernment since it can result in a risk of invalidating for certain administrative decisions. This indicates why not all the legal solutions that have been applicable to eCommerce services can be automatically put into practice in the field of eGovernment.

These reasons may also explain why no direct references to Adminstrative Law have been found in the numerous documents on eGovernment analysed, most of them obtained from official EU websites. Consequently, we must focus our attention on the legal initiatives carried out by Member States. Some States have passed overall eGovernment legislation in addition to the EU's general legal framework on ICT matters (e.g. eCommerce, digital signature and data protection). As shown at website[105] of the European Commission's IDABC programme to promote eGovernment in Europe, only Austria, the Czech Republic, Finland, Italy, Latvia and Slovakia have adopted this approach. Several other states (e.g. France, Slovenia and Spain) are in the process of preparing their eGovernment laws, which are due to be passed shortly. Analysis of these regulations is important to discovering whether they have overcome the existing barriers to eGovernment posed by Administrative Law or, on the contrary, have led to the appearance of new obstacles.

Certain European initiatives have had a direct impact on the field of Administrative Law since the existence of a specific – and singular – framework for public administration is closely related to some of the principles of the European common market. Specifically, particular administrative requirements may not only hinder the effectiveness of its administrative activity but also become a serious barrier for the competitiveness of the EU economy and European companies. Thus, any project for the technological modernization of public administration must take into account the ways electronic services provide a unique chance of simplifying administrative procedures, especially in terms of both data input by users and documentation to be provided[106]. Here, the *French eGovernment Strategic Plan*[107] offers a relevant example as one of its main aims is to promote 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

[105] http://europa.eu.int/idabc/en/chapter/383

[106] A report published by the Danish Commerce and Companies Agency (*Better E-governance. A Measure of E-governance in New Danish laws*) has noted that most of the hindrances to eGovernment introduced by the analysed laws were formal requirements.

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

eGovernment services. This includes the introduction of a new bill on administration simplification to be presented to the Parliament by the Minister in charge of State Reform, which will include an item on eGovernment.

Finally, the consolidation of pan-European electronic services can also cause barriers at the national level since, although Administrative Law mostly remains a national prerogative, it has a major impact on eGovernment at the European level because those services are usually based on the activities – and therefore their legal limitations – of national, regional and local public administrations and their information systems. Underestimating, or not accounting for, different models of legal frameworks for public administrations can therefore be considered a serious potential barrier for the actual take-up and future expansion of pan-European eGovernment services.

4. What is the relationship of this legal area to the seven barrier categories?

The following discusses each of the barrier categories highlighted in Part 3 to analyse their relevance to Administrative Law.

Leadership failures: *Somewhat Significant*, since the lack of adaptation of administrative legal frameworks to the requirements of ICT may come about because no leadership is given in taking special account of eGovernment perspectives, including in relation to legal dimensions.

Financial inhibitors: Somewhat *Significant*. Although there is no a direct relationship with this barrier, it may occur that the existence of a specific legal framework for public Administrations demands certain adaptations of the electronic means to them and, therefore, a higher investment should be required. Anyway, this inconvenience can frequently be removed with minor modifications of the present regulation when it is not appropriate for the exigencies of technology. Moreover, sometimes a *modern* interpretation of the *old* provisions bearing in mind the singularities of ICT can be enough to solve that problem.

Digital Divides: *Not Significant.* The difficulties of certain groups to access to eGovernment services are not connected to the existence of a singular legal framework for public Administrations since, usually, they are produced by economical, cultural or technological circumstances that are not related to the regulation of the activity of those public Administrations. However, a wider access to digital networks could be promoted in some cases by public authorities if there were not so relevant obstacles from the perspective of Competition Law, which can not be identified with the requirements of Administrative Law.

Poor coordination: *Significant*, for two main reasons. Firstly, ICT-related EU Directives (e.g. digital signatures, data protection and eCommerce) do not take sufficient account of the singularities of public administration in many of the Member States, especially those belonging to the continental model. On the other hand, technological adaptation of Administrative Law usually requires an effective coordination among all public administrations concerned, especially when national authorities have the competence to promote general modifications in this field which must be respected at regional and local levels.

Workplace and organizational flexibility: *Very Significant*, as one of the most important challenges to introducing ICT in this field is to make the most of the technology's potential strength in helping to modernize and improve administrative activity. However, this opportunity will not be realized if traditional legal obstacles remain unreformed. This is particularly relevant when the necessary simplification of administrative procedures is not undertaken and digital information is used instead of traditional paper-based documents.

Lack of trust: *Significant*, because the lack of adequate adaptation of traditional regulations based on personal and direct contact between citizens and public bodies may hinder the technological innovations offered by eGovernment to improve the quality of public services, particularly if citizens and companies are concerned that eGovernment provides a lower degree of legal security (e.g. through the automation of decisions and the nature of constraints imposed by the demands of formal administrative procedures). A similar problem also appears when technological regulations do not bear in mind the singularities of administrative activity from a legal point of view, as occurs the field of data protection, digital identification cards or eCommerce.

Poor technical design: *Not Significant*. Some Member States have established legal obligations for public Administrations in order to provide access to eGovernment services in good conditions from the perspective of technical design, particularly for websites and access to administrative information. Nevertheless, the existence of a specific legal framework for public Administrations can not be considered an obstacle when trying to achieve an adequate technical design for eGovernment services: this objective should be always pursued, even when there are no specific provisions.

5. What are the barriers remaining in this field?

5.1. Constraints of administrative procedure requirements

One of the main goals of Administrative Law is to ensure that administrative decisions must be adopted through the appropriate procedure; laws that have been 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. The importance of procedure is certainly relevant since, except in some very isolated cases, all unilateral decisions with legal implications must respect this regulation. There is a double justification for this requirement: an appropriate satisfaction of public interests, and a guarantee for citizens against administrative decisions that are usually taken in the exercise of very powerful and unilateral competences. Therefore, as in the field of judicial procedure, the correct observance by public administrations of a legally predetermined sequence of steps must be considered as a useful and necessary tool for adopting decisions in an objective and fair way.

The implementation of electronic public services demands a higher level of streamlining and flexibility of rules and procedures than for traditional methods in order to realize fully the potential benefits of using ICT to enhance efficiency in decision making and in establishing communications with citizens and companies.

For eGovernment services, these operations could be done automatically without a formal procedure or, instead, by following a more informal process than that fixed for those actions when carried out using traditional tools based on written documents and personal relationships. If the legal framework does not admit these 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.

It is therefore necessary to promote a review of this legal framework in the light of relevant technological change in order to avoid these negative consequences for the implementation on eGovernment services. Although this process is generally the responsibility of national authorities and, depending on the context, of regional and local governments, in certain cases the EU may influence the outcome positively when it has the competence to act in a particular field. For instance, the potential benefit of such a European influence has been clearly shown by Directives 2004/17/EC and 2004/18 on public procurement. This EU-wide regulation has been rapidly taken into account by many Member States, such as in France's adaptation of its own legal framework that goes even further than recommended by the Directives[108]. With a more general scope, the need for simplifying administrative procedures has also been advised as a trend in public needs for eGovernment services by the Report *eGovernment in the EU in the Next Decade: The Vision and Key Challenges* (Institute for Prospective Technological Studies 2004)[109].

Some other relevant general initiatives in this area include: the European consultation on 'cutting red tape' and the projects to reduce 'administrative burdens' launched by several Member States, including Sweden[110], The Netherlands[111] or Denmark[112]. Such simplification of administrative procedures is one of the main priorities of citizens in those States with a continental model of public administration, as recently shown in France[113]. This indicates that technological modernization of public administrations should be used to simplify the design of administrative procedures to make the most of this historic process, which involves much more than a question of changing from a paper-based format to a digital media. The success of eGovernment from a legal point of view requires taking account of the importance of avoiding the establishment of harder constraints on administrative activity when using ICT tools, unless such a course is reasonable in a particular context.

Regarding the measures to overcome this inconvenience, administrative rules based on traditional and well-established legal principles are usually neither designed to promote the use of ICT nor prepared to allow it, since the appropriate technological innovations were merely imagined when the laws were passed or rules made. There may even be some provisions that are contrary to the use of ICT, such as a

[108] As explained in the country examples of eProcurement section of our project's website: at http://www.egovbarriers.org/?view=example&example=procurement
[109] http://europa.eu.int/idabc/servlets/Doc?id=19131
[110] http://europa.eu.int/idabc/en/document/4362/330
[111] http://www.administratievelasten.nl
[112] http://www.amvab.dk
[113] According to a survey by BVA (http://www.bva.fr), 60% of those polled declared this should be the main priority for public administration. Further information about this question can also be found at http://europa.eu.int/idabc/en/document/4501/194

requirement for the use of certain types of paper document[114], which create a clear and significant barrier. At the same time, there can be a more positive approach to technological change if a legal silence on technology could be interpreted as an implicit authorization. Therefore, it is always necessary to asses if a legal modification must be promoted to solve these problems or whether, on the contrary, only a different perspective is enough to overcome a perceived potential blockage to eGovernment (Johnssén 2003). To avoid this kind of uncertainty, Italy has recently passed broad legislation on eGovernment, the 'Codice dell'ammnistrazione digitale'[115], that aims to contribute to removing 'obsolete norms' as an obstacle to further eGovernment development.

Consequently, when a modification of the legal framework is essential in order to adapt obsolete rules, it will be necessary to check which kind of decision is required and the relevant competent authority to promote it. If the regulation has been approved through a general Act, then a Parliamentary intervention will be indispensable, thereby involving a higher complexity in which the public administration concerned will not be able to overcome the barrier on its own. On the other hand, a rule whose modification has only an administrative range will be easier to change, especially if the competent authority belongs to the same public administration that is encountering the obstacle.

5.2. Inadequate adaptation of administrative decisions by the competent authority

Following on from the previous section, it is also important to note the latent tension between the possibilities offered by ICT means and the formal requirements of Administrative Law. This poses a potentially serious barrier to which the general points made in the preceding section also apply. A clear demonstration of this confrontation can be seen in the legal conditions for the validity of administrative decisions, most of which require compliance through a paper-based document and with the direct intervention of a person and not a machine.

This indicates why the validity of administrative acts can be questioned when using ICT, since the observance of some essential formal demands may be impossible or, in some cases, contrary to the flexibility and speed offered by technology (Girot 2002). In this context, a relevant risk for eGovernment can be seen to arise in some circumstances when it is not possible to place administrative decisions using digital media on the same level of validity and efficacy as those adopted by traditional means. The scope of this inconvenience and complexity of dealing with it are illustrated by some related questions, such as: Can administrative decisions be 'adopted' by a computer? Which kind of decisions? Although it is obvious that discretionary powers must be put into practice directly by the competent authority, what are the limits for other public bodies dealing with an issue? Is it necessary for a person to draw up a death certificate?

One of the main conditions for the validity of administrative decisions is that they are adopted by the competent authority, which can be identified with a natural person who assumes the consequences of his/her action. This principle in the field of Administrative Law may be considered a relevant barrier for the implementation of

[114] This is the case with the Spanish Act on Legislative Promoting.
[115] Further information on this example can be found at http://europa.eu.int/idabc/en/document/4820/5707

eGovernment services because many decisions could be taken directly by ICT-enabled systems without a direct human intervention. Even more, from the point of view of the responsibility for the decision adopted, the use of ICT involves an essential problem of determining who must be considered the author of the administrative act and, therefore, responsible from a legal perspective (Marcou 2002). This raises inevitable questions about the legal conditions required to automate administrative activity, the strict limits that have to be respected if administrative decisions are to be considered valid and, if necessary, how to promote those legal modifications demanded by electronic public services.

Overcoming this obstacle requires a specific framework taking account of the singularities of eGovernment that could not be have been considered when the rule was formulated as that technology was not yet available, which meant administrative activity was based on the use of paper and through personal relationships. The Spanish basic *Act on Administrative Procedure*[116] offers a relevant example of the legal conditions imposed on the use of ICT in order to enable all public authorities at national, regional and local levels to exercise their competences. It includes a demand for prior approval by the competent authority of the software used for this purpose, who must publicize its technical characteristics. Thus, a direct link can be established between that authority and the administrative decisions adopted through electronic means. Nevertheless, in this case an alternative solution may be pursued if there is no clear regulation related to this problem. Instead of adapting the current framework, public administrations can avoid the obstacle to validating administrative decisions by interpreting the general rules according to the requirements established by this Spanish Act. However, this is a hazardous solution from the legal security point of view and, in the last analysis, could subjected to a judicial review to assess the fairness of the approach followed.

5.3. Failure to reduce the administrative burdens relating to the conditions of administrative documents

As already indicated, one of the main concerns of European and national authorities regarding Administrative Law and eGovernment is to simplify the requirements for easing the so-called administrative burdens, particularly those aspects involving the inevitable exchange of information that demands the kind of networked operations highlighted as one of the main challenges to eGovernment in the Report *eGovernment in the EU in the Next Decade* (Institute for Prospective Technological Studies 2004).

This is not only a question of efficacy from an internal administration perspective. It is also a relevant barrier when implementing inter-administrative electronic public services, where there can be an even wider significance if the potential problems are not addressed successfully. Such inconvenience could be increased in the field of pan-European electronic services[117], where information is provided by diverse public administrations subjected to heterogeneous legal frameworks that impose different requirements for administrative documents. The external conditions within which such services are designed, developed and used can be as important as the content

[116] This Act and other regulation related can be found at http://www.map.es/documentacion/legislacion/procedimiento_administrativo.html

[117] This was one of the most relevant topics examined in the small group discussion held in Brussels at a *Breaking the Barriers to eGovernment* project workshop on 29 September 2005.

of those services, for example in terms of legal tradition and culture not only the validity of particular ePublic Services (Yahiel 2002).

This indicates why the electronic exchange of administrative documents must respect any formal legal requirements to establish their validity and efficacy. If this is not done, the advantages of using electronic media will be counteracted by the legal conditions. It is therefore necessary either to simplify the formal requirements, which is not always a feasible option, or – as a better option – to establish an alternative way of providing the specified level of guarantee for the information contained in the documents in a way that has been fully adapted to the capabilities of ICT tools.[118]

This has been the option assumed by the Spanish *Act on Administrative Procedure*, which allows substituting traditional formalized written certificates for simple online transmissions of the information they contain. As this does not require any legal change, it can be adopted by each public administration provided adequate technical measures are used, such as digital signatures and secured channels that guarantee the authenticity and integrity of the information[119]. A different solution has been adopted for certain pan-European services, such as the EURODAC[120] centralized database for asylum application, which is based of the flexibility offered by Article 1.2 of Directive 95/46/CE for international exchanges of personal data. However, this option is not always possible at the national level if local legal limitations make it difficulty to meet the requirements for implementing effective eGovernment services.

5.4 Lack of adaptation of technological regulations to the singularities of Administrative Law

Several relevant EU Directives have sought to modernize national legal frameworks in order to adapt their regulation to the special needs of the information society, especially in the fields of digital signatures and eCommerce. In this process, a strong influence of Private Law can be seen as a consequence of two main circumstances: this new regulations has been adopted with the clear economic purpose of facilitating the common market in certain sectors; and these Directives have an effect on equivalent regulations in North American, which has a legal system where Administrative Law does not have a significant role. As a result, these Directives either have not included specific provisions for public administrations or their provisions are not sufficiently adapted to their particular needs from a legal perspective. This has made it necessary to apply private rules to the general process of technology change in public administration systems (Gautier 2002). These conditions may become an obstacle to the development of certain eGovernment services, for instance when a Member State has to adapt its national regulations to the requirements of these Directives, although Private Law principles may not be adequate enough for the administrative legal framework.

[118] At a basic technological level, this demands the interoperability of the software used by all the public administration concerned. See Part 4, Valero Torrijos, J., 'Relationships between Administrations, Citizens and Other ICT Actors'.
[119] Unless specific demands are imposed by regulations applicable to certain documents.
[120] EURODAC involves a centralized database in comparing the fingerprints of asylum applicants and a system that enables each Member State to transmit data to this central record. For further information about this, see: http://europa.eu.int/scadplus/leg/en/lvb/l33081.htm

An illustration of difficulties that can be encountered relates to the provision in the Directive on digital signatures for a free certification service. This means that citizens and companies could use the certificates supplied by a service provider established in their own country in order to contact a public administration belonging to another Member State. However, although this Directive allows for some exceptions to its general rules for the public sector, certification has not yet been put in action generally due to the singularities and diversity of each national administrative context and the very important problems related to a lack of interoperability. These obstacles should be overcome by a future modification of the Directive that fixes clearer conditions for exceptions in the administrative field. Meanwhile, they can be solved by national authorities on the basis of the priorities of European Law.

On the other hand, the Directive on eCommerce is not applicable to public administrations, since its conceptualization of 'service' does not include public services. From this perspective, the limitations of liability for intermediary service providers does not affect those services offered by public administrations. This situation could be worrying to those States whose administrative systems are based on the direct and objective liability of public administrations. To address such concerns, national regulations should adapt the internal framework to the demands of this Directive to ensure public administration is subject to the same regimen as private intermediary service providers.

5.5. Failure to preserve guarantees to citizens when moving to the use of electronic media to deliver public services

The tension between administrative efficiency and the protection of the rights of citizens and companies when adapting Administrative Law regulations to the specific requirements of using ICTs can result in an over-emphasis on the needs of the public authorities that dominate regulatory and legal decision making. A lack of adequate adaptation also carries a risk, since many of the traditional rules take account only of personal contacts but not online communications (Prins 2002).

Administrative Law may be ignored if it is not suited to the concrete and real circumstances in which it must be applied. This could give a greater weighting to technological capabilities over citizens' rights in implement eGovernment services (Lessig 1999), which would be disadvantageous for citizens and companies when they engage in online relationships with public administrations. To ensure that the rights of citizens and businesses when using electronic media are guaranteed at least to the same level as if traditional means were being used, regulations relating to interactions with public bodies must therefore be adapted appropriately to take specific account of the use of ICT-based tools. If there is an unfair lowering of the level of protection when using electronic media, many citizens and businesses could lose interest in eGovernment services, even for those from which they could benefit substantially.

For example, in the past when a citizen wanted to address an application form to a public administration, he/she would typically have had to go to an administrative building and to the appropriate desk, where a civil servant would issue a receipt to prove the document has been handed over and, if necessary, give a warning if there are certain problems with the form. When that action is made through Internet, there is no direct personal response since nobody is waiting on the other side of the Net.

On the other hand, when a public administration wants to notify its decisions to relevant parties, the specific rules regarding this kind of administrative communication must be observed since the effectiveness of those decisions may be affected, for instance when the specification of a time-scale to lodge a judicial appeal does not start until the notification has been correctly made.

Consequently, public administrations should be legally obliged to give all the necessary information online in order to deal adequately with application forms delivered through electronic means, particularly when that possibility has been recognized as a right. Administrative websites must warn citizens and businesses of any mistakes during this process and an immediate digital receipt must be drawn up and delivered to the relevant party. For notifications of administrative decisions, the absence of a personal contact demands a particular legal regulation to guarantee the correct reception of this kind of communication, especially to indicate the consequences of a technical mistake when trying to undertake the necessary actions notified. Public administrations can adopt these measures even if there are no legal obligations to do so, but in such cases citizens will not have their rights protected at the same level as when using an alternative to eGovernment services.

5.6. Restrictions on multi-channel access to eGovernment services

The use of electronic means may offer significant advantages for citizens and companies compared to more conventional channels. However, this can also threaten the achievement of inclusivity and equity goals as it could exclude many who do not have the finance, skills and support to enable them to make effective use of eGovernment capabilities. This could be a real barrier if there is compulsory use of ICT, but otherwise it could be regarded as a *perceived* legal barrier with social and/or economic implications since it may not be possible to establish direct legal consequences if the decision about whether to use electronic public services or more conventional ones is regarded as a voluntary choice.

However, there is a clear exception when a public administration decides to use electronic means to speed up its processing of applications through the use of ICT because the information needed has already been processed or can be collected faster. In such cases, it would be desirable to fix some specific legal limits, especially where other citizen's rights may be affected, such as in competitive procedures relating to the awarding of financial subsidies. Although a clearer regulation should be adopted, this kind of problem could also be easily solved without any legal reform, as it could be sufficient to apply current rules in a prudent way. Moreover, in certain cases this kind of problem can be overcome through purely organizational measures, such as enhancing the personal face-to-face service provided at the traditional administrative office in order to give the same information as offered through the Internet.

6. Analysis and assessment of the main Administrative Law research questions from a legal perspective

Our analysis to date of the implications of eGovernment developments for Administrative Law has identified the following key relevant and concrete questions whose answers could help to better understand which legal measures could help to avoid or overcome obstacles that could hinder the development and consolidation of

eGovernment services. A more in-depth analysis of these issues will be undertaken during the remainder of this project.

6.1. Are different government legal–administrative frameworks discouraging or failing to promote the use of electronic communications with – and within – government?

The provision of eGovernment services to citizens and companies established in other Member States is much facilitated when there is a uniformed legal framework across Europe. Although some Directives and other European regulations have already sought to establish a minimum level of harmonization in some essential fields, such as data protection, public procurement and digital signatures, there are still some relevant divergences not only in the specific regulation of each country but also in the interpretation and implementation of the European rules. This was illustrated by the way the availability of certification service providers established in a different European country to the one where the public administration that offers the services is located poses problems, such as difficulties in validating the status of the certificates. Other inconveniences may also appear when eGovernment services are provided to other public authorities, particularly in the field of data protection where the diversity within national regulations may make it difficult to exchange information between authorities in different Member States.

6.2. Does eGovernment need Directives more analogous to the eCommerce Directive (2000/31/EC), in which the concept of 'service' does not include public services?

Regulating the activity of public administrations mostly remains a prerogative of Member States as there is no general competence for this reserved to the EU, although there are some European regulations with a direct influence in this sector (e.g. public procurement of environmental protection services and technologies). In addition, ICT-related Directives with specific rules for public bodies do not usually impose a strong degree of uniformity. On the contrary, when Directives like 2000/31/EC on eCommerce keep silence about their application to public administration, a serious risk of uncertainty arises from the legal perspective. Therefore, it would be preferable to set a minimum specific provision for public bodies, which may be developed – or left at the minimum level – by each Member State, according to their own legal singularities and traditions.

6.3. What are the problems in specific relationships between different governance levels (e.g. between Member States and regions or Member States and the Commission)?

From the European perspective, the lack of a general competence to approve regulations regarding public administrations is a relevant inconvenience that may also appear at the national level. In this field, another potential legal obstacle to developing networked services can appear if, for political reasons, national authorities sometimes do not exercise their powers to establish more uniformity in relevant regional and local regulations. The constitutional autonomy of regions and local bodies could be another relevant obstacle, as this can constrain certain administrative and organizational decisions designed to promote the use of

electronic means, such as approaches based on a wide understanding of a citizen's right to use ICT to contact relevant authorities.

Some problems that were previously perceived primarily as being at the international level must also be considered as national scenarios, since the divergence of regional and local administrative regulations may become a serious obstacle to exchanging information in an effective way. Sometimes this situation demands general measures that must be adopted by national authorities, who may not have a clear competence for this purpose or may not want to exercise it to impose legal solutions that are the responsibility of regional and local powers.

6.4. To what extent have administrative laws in different Member States constrained or blocked the required simplification of requirements for networked eGovernment services that are necessary to lessen the 'administrative burden'?

One of the main problems in providing eGovernment services across Europe is that sometimes it is essential to prove certain facts or circumstances through documents drawn up by a public authority from another Member State, which is subject to different formal and substantive requirements than those fixed by the regulation of the country in which the service is demanded. Since there are no overall EU criteria to solve this kind of international problem, general rules should be adopted in order to clarify which regulation has to be applied when there is no clear and specific solution. A greater effort should also be made to harmonize the elements of public documents across Europe and to substitute paper-based documents by online exchanges of information.

From a national perspective, there should be legal guarantee not to have to have to present paper-based versions of those documents that are already in the possession of the public administration that offer the electronic service. In order to simplify the procedure and not to force users to act as intermediaries between public administrations, public bodies could also ask for the authorization of citizens and companies through electronic means to facilitate the exchange of necessary information to exercise their competences.

6.5. Are there cases at the Member State level where an inadequate, or complete, lack of adaptation of Administrative Law to new technological contexts acts as a barrier to the development and take-up of eGovernment services?

A general requirement for the validity of administrative acts and decisions must be their adoption by the competent authority relevant to the field concerned. This requirement may not be respected when putting into action eGovernment services, since some decisions need to be made directly by a computer in order to achieve a higher efficiency. Many administrative regulations have been conceived and formulated for implementation through paper-based processes and personal relationships, which often mean they cannot be interpreted directly for application in an ICT-enabled environment. It is therefore likely that many traditional administrative regulations need to be adapted to avoid the negative consequences of a judicial review that may consider a public decision to be invalid if it does not offer a comparable level of guarantee with those adopted through traditional means.

Moreover, in certain cases more modern regulations – such as ICT-related Directives and national laws on digital signatures – may also be not suitable from this perspective, for example if the use of digital certificates is legal only for natural persons and not for computers and automated processes. A clearer regulation regarding this potential obstacle should aim to avoid offering such a conditions, as it could hinder one of the main legal requirements for eGovernment services: the authentication and integrity of ICT systems and digital documents.

Authentication and Identification in eGovernment

Dr. C Cuijpers and Dr. J. Nouwt, Tilburg Institute for Law, Technology, and Society (TILT), University of Tilburg, Netherlands.

1. Description of the area

The topics that are being described here are 'authentication' and 'identification'. 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 information. Identification is an act of establishing or confirming the identity of a person. The difference can be illustrated by the example of someone logging in to a shared account on a computer, who will not be uniquely identified but can be authenticated as one of the users of the account through the use of a shared password. On the other hand, identification does not necessarily authenticate the user for a particular purpose.[121]

Authentication is used for the procedure of guaranteeing the origin and the integrity of electronic information.[122] A "digital signature" can be used to secure electronic information in a way that enables both the originator and the integrity of the information to be verified,. This is a type of electronic signature that uses public key cryptography in which the author of electronic information can "sign" this information with a secret cryptographic key. This key must always be kept private by the user. The signature can be verified only with the associated key of the author that has been made public, so is known as the "public key". This authentication procedure is therefore a confirmation of the identity by proving the possession of a secret key, which the author has used to encrypt the information. The recipient checks the identity of the author by decrypting the information with the public key of the author.

Authentication and identification can be considered elements of a broader concept: "identity management", which arises because of the need for governments to authenticate online users [NECCC 2002, p. 35]. As authentication is needed to avoid or reduce the risk that the wrong person will access, use, change, delete or otherwise improperly interact with valuable data or transactions, authentication and identity management can be considered elements of legal risk assessments and risk control measures.

2. Why might this legal area be related to barriers to eGovernment?

Many non-electronic transactions between government and citizens or businesses are concluded with a signature, such as to authorize receipt of a welfare payment or sign a cheque. When services are moved to the electronic world, the need emerges for an equivalent electronic means to ensure: 1) the authenticity of each party within the electronic communication; 2) the integrity of the contents of the communication; 3) the electronic communication can be confirmed if there is a dispute.

---

[121] RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1. Chapters 2.2.2 and 2.2.5. On the Internet: http://www.rsasecurity.com/rsalabs/node.asp?id=2152

[122] J. Dumortier, Directive 1999/93/EC on a Community framework for electronic signatures, in: A. R. Lodder and H.W.K. Kaspersen (eds.), e*Directives: Guide to European Union La won E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection*. The Hague/London/New York: Kluwer Law International, 2002, p. 33-34.

The process of authentication relies on the accessibility of the public keys of the users to all the communication partners. It also relies on the trusted relationship between the identity of the users and their public key. Furthermore, the authentication procedure is based on the presumption that the public key really belongs to the signer. There is a risk that somebody creates a key-pair, places the public key in a public directory under somebody else's name and signs electronic messages in the name of somebody else.

Another risk is that the public key does not belong to the claimed identity, as a public and private key pair has no inherent association with any identity because it is simply a pair of numbers. To limit these risks, there are third parties that certify public keys by guaranteeing the relationship between the identity and the public key through the use of a "digital certificate". The third party is called a "certification authority". It is important that the third party is accepted by all users as impartial and trustworthy.

A significant barrier to the use of electronic communications and electronic commerce and government may be created by divergent national rules with respect to the legal recognition of electronic signatures and the accreditation of providers of certification services as being able to offer these signatures. In this respect, the primary aim of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 is to create a "harmonized and appropriate legal framework for the use of electronic signatures within the Community and to establish a set of criteria which form the basis for legal recognition of electronic signatures". However, it is at least necessary to: further clarify the open norms laid down in the eSignatures directive; and examine how theory and practice can be better tuned and whether the law can create solutions to overcome obstacles relating to the balance between costs and benefits in the use of digital signatures.

According to the report *The Legal and Market Aspects of Electronic Signatures*, Directive 1999/93/EC sets very high requirements on secure signature-creation devices.[123] Such devices still rarely find their way to the market. The authors plead for more flexibility for these legal requirements in the future. Otherwise, the high legal requirements could be a barrier to eGovernment.

However, there is a general question about whether such legal requirements are real barriers for eGovernment initiatives. Failure to meet legal requirements does not necessarily prevent someone from taking the first step to eGovernment initiatives. Initiatives can be taken and eGovernment services can be delivered even when the initiative is not fully in compliance with the law. The initiator can deliberately take the risk that the initiative will be taken to court, with the service being delivered, as long the case is not ruled illegal in court.

Nevertheless, divergent national rules with respect to the legal recognition of electronic signatures and the accreditation of certification-service providers may create a significant barrier to the use of electronic communications and electronic commerce and government.

[123] J. Dumortier and others: *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*, p. 11.

3. What is the European context for this area, including legislation, policy statements, institutional arrangements relevant to this topic?

On 13 December 1999, Directive 1999/93/EC on electronic signatures was signed, and published in the Official Journal of 19 January 2000. From that date, the EU member states had 18 months time to transpose the Directive into their national law.[124]

This eSignatures Directive is an example of co-regulation at European level. The Directive itself defines only the general principles, which must be further specified by self-regulatory mechanisms, mainly by technical standardization. At the end of 1998, the European Commission issued a mandate to the European standardization bodies (CEN/ISSS, CENELEC and ETSI) to analyse the future needs for standardization activities in support of essential legal requirements related to electronic signatures products as stated in the (then draft) directive,. To meet the requirements of the Commission mandate, the ICT Standards Board (ICTSB)[125] launched the European Electronic Signature Standardization Initiative (EESSI), which published in July 1999 an expert report about future standardization requirements at a European level. Based on this report, EESSI approved a work programme with a division of tasks between CEN and ETSI. In the months that followed, intensive work has been performed in the area of standardization of electronic signatures, with a first set of deliverables given to the European Commission on 3 April 2001.

References to the required standards were published in the Official Journal in July 2003. These are part of a longer set of specifications defined by EESSI and are included in their work programme. With the publication of this full set of standards, EESSI has fulfilled its mandate and consequently ICTSB decided to close EESSI WG in October 2004.[126] However, standardization work in this area is still ongoing by CEN members, and by ETSI TC/ESI, but at a lower level of activity,. Remaining co-ordination tasks in the area of electronic signatures are now carried out by the Network and Information Security Steering Group (NISSG) of ICTSB.

The existence of a European legal framework regarding digital signatures is no guarantee that this field of law no longer entails any barriers to eGovernment. In this respect, reference can be made to an earlier study conducted for the European Commission – DG Information Society – under the lead of Jos Dumortier: *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*. This report shows that much work still needs to be done in the field of electronic signatures before a pan-European use of these signatures can be expected. For example, divergent rules still exist within the European Community because of different interpretations regarding the eSignatures directive.. The report concludes that the text of the Directive is adequate enough to serve its purpose in

[124] J. Dumortier, Directive 1999/93/EC on a Community framework for electronic signatures. In: A.R. Lodder and H.W.K. Kaspersen (eds.), e*Directives: Guide to European Union La won E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection*. The Hague/London/New York: Kluwer Law International, 2002, p. 39.
[125] For more on ICTSB, see http://www.ictsb.org
[126] See: http://www.ictsb.org/EESSI_home.htm

the near future, but that it needs re-interpretation and clarification. A subsequent conclusion of relevance to our project is that without this re-interpretation and clarification, barriers to eGovernment will remain with regard to eSignatures. Clarification is needed, for example, with regard to supervision schemes, voluntary accreditation and the public sector exception. National rules regarding the recognition of foreign qualified certificates may also still pose a barrier to eGovernment across state boundaries.

In some instances, the report even explicitly refers to eGovernment [Dumortier 2003, p. 12]: “It is necessary to perform a more detailed study on the Internal Market consequences for eGovernment programmes of the Member States. There is a clear danger that these programmes will result in national barriers, fragmentation and interoperability. Efforts towards improvement of interoperability between eGovernment programmes and particularly between their electronic signature applications should be supported or initialized at a European level.”

Another interesting point in the report was the conclusion that a clear need exists for regulation dealing with archival service providers, or with registered mail services. From a user’s perspective, it is difficult to understand why such services remain completely unregulated, while a complex regulatory framework has been established for issuers of certificates. It is therefore recommended to undertake studies about the need for regulation with regard to other categories of trust services. In this respect, reference can be made to the First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular eCommerce, in the Internal Market Directive on electronic commerce[127].

A central source of disagreement among scholars and lawmakers is about whether the laws governing electronic signatures should remain neutral towards technology or attempt to specifically regulate currently favoured technologies. In this respect reference can be made to the following statement of Andrew Barofsky, “Digital signatures are not the only available form of secure electronic signature. ‘Signature dynamics’ combines biometrics and cryptography to create signatures that securely attach unique characteristics of an actor’s character or behaviour to an electronic document. Signature dynamic methods of authentication have the advantage of being bound to the signatory rather than to the document. This feature eliminates the need to go through a trusted third party or a CA to link an electronic signature to an individual. Favouritism toward digital signatures risks excluding other possibly superior technologies from entering and competing in the marketplace.”

The main problem is that in jurisdictions that have enacted laws specific to certain digital signature techniques, it is not clear whether an electronic message signed by any method other than a digital signature is valid. Under the current eSignature directive, a business using an otherwise “secure” signature method that is not a digital signature subject to a qualified certificate risks creating an unenforceable or voidable contract. This problem is aggravated by the fact that businesses as well as government, choose methods for signing their computer documents that meet their commercial needs. For the Netherlands, mention can be made of DigiD (Digital Identification), started on 1 January 2005. This employs a username and password

[127] http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2003/com2003_0702en01.pdf

systems to identify citizens when they access online eGovernment services. However, questions have been raised about whether it complies with the requirement for an advanced eSignature, for example with the Dutch Society of Information Security (GvIB) reporting in April 2006 that it is too weak a mechanism of authentication to make it appropriate for application to tax forms.

A final point to mention is that high standards required by the Directive with regard to digital signatures has led to a system in which the costs do not outweigh the benefits. This is true not only for customers, but also for certification service providers. In theory, therefore, although the digital signature system may seem to be efficient, in practice its complexity and cost could be its drawback and a potential blockage to some eGovernment developments.

At the Workshop on Digital Identity [Camp 2003], seven critical problem areas for an identity management discussion have been identified.

- information architecture and management strategy;
- privacy and personal information protection;
- governmental policies;
- accountability inside and outside the system;
- metrics for design and evaluation;
- implementation of the infrastructure; and
- roll-out and enrollment phase.

Each problem area has many independent and related research topics. Together, these make up a research space in which each problem area offers many individual questions to be addressed, both qualitatively and quantitatively. Camp subdivides these topics into six academic disciplines: Computer Science and Engineering; Management Information Science; Organizational Science; Economics; Social Sciences; and Law. For the legal discipline this means that significant changes to current authentication practices will implicate current legislation on individual rights, administrative responsibilities and organizational liability burdens [Camp 2003, p. 25].

4. What is the relationship of Authentication and Identification to the 7 barrier categories and associated research questions?

4.1 Leadership failures

At first sight, the issue of authentication and identification does not seem to be relevant for this category of barrier. However, a lack of leadership could result in slow development and implementation of authentication and identification processes. This is illustrated by examples from different countries. For instance, from 2003 a Certificate of Residence can be obtained electronically in Austria by using an electronic signature on a smart card. Despite advances in technology, an online

authentication technology like DigiD, which is being used in the Netherlands, has been criticized as being unfit for some eGovernment purposes Knowledge and vision on technological developments seems to be important elements for leaders to guarantee the use of state-of-the-art authentication and identification processes.

4.2 Financial inhibitors

The use of a secure electronic signature, or even the combination of electronic signatures with biometrics, could be rather expensive. It seems clear that higher security demands result in higher costs for authentication and identification. In this context, a relevant question is whether the costs of providing effective security and trust systems could outweigh the benefits by raising the overall entry point for affordable investments?

4.3 Digital Divides

Authentication and identification processes should be easy to use and not too expensive to apply, so a process like a digital signature should not be too expensive for an organization to apply or too difficult to be used by any of its customers. Otherwise, a digital signature could result in digital divides.

4.4 Poor coordination

As illustrated above, despite the existence of Directive 1999/93/EC on electronic signatures, a lot of work needs to be done to establish a pan-European use of electronic signatures. Within EU Member states, different rules still exist because of different interpretations of the Directive provisions. This has also resulted in the failure to agree and implement standards for electronic signatures. Therefore, despite the harmonization efforts attempted through several Directives, the following questions need to be discussed:

- Are there provisions in Directives that hinder the effectiveness of administration activity at different levels or have become a barrier for the competitiveness of the European economy, and how can they be altered to remove any blockages?

- Has the European framework on electronic and digital signatures achieved greater trust in secure information exchanges by overcoming critical variations across the EU? If not, what further initiatives would be required?

4.5 Workplace and organizational inflexibility

When authentication and identification processes are introduced in an organization, management and staff could resist such innovations. In some cases, their resistance could be legitimized by laws. For example, when the introduction of authentication and identification processes result in the processing of personal data from employees, the consent of the relevant Works Council could be needed. More generally, the question is raised about ways in which the current structure of Employment Law in Member States act as a blockage or facilitator for any restructuring of the public sector labour market that may be needed to realize the full benefits from high levels of ePublic Services delivery and use?

4.6 Lack of trust

As in eCommerce, trust seems to be an important enabler for eGovernment, especially because governments often process highly sensitive personal data from their citizens. Therefore, it is also of great importance that access to those personal data is highly secured with advanced authentication and identification procedures. In this context, the following research questions will be addressed:

- What delays in eGovernment developments have been caused by an absence of standards in approaches to identification of an individual or other unit – and the verification or authentication of that identity – which is essential to public service transactions, such as receiving welfare benefits, voting or paying vehicle-related charges? What blockages need to be removed in order to establish standards of identification and verification for pan-European online services?

- What obstacles have there been to wider use of electronic and digital signatures, in addition to any harmonization issues across Europe?

- How does fear of identity theft, fraud or error affect citizens' willingness to use eGovernment services?

4.7 Poor technical design

The report *The Legal and Market Aspects of Electronic Signatures* recommends the standardization of the European "Qualified Electronic Signature", which should give users a presumption that an electronic signature that complies with this standard will be presumed equivalent to handwritten signatures throughout Europe.[128] Such a Qualified Electronic Signature would be especially useful for cross-border transactions in Europe. Therefore, in this context the question will be addressed: Does a lack of standardization or interoperability of electronic identification and authentication technologies remain a barrier to eCommerce applications in the public sector?

5. What are the real and perceived barriers remaining in this field?

In this section we use the working definition of a barrier defined for this project (see Part 1):

Characteristics – either real or perceived - of legal, social, technological or institutional context which work against developing eGovernment at the EU level, either a) because they impede demand, by acting as a disincentive or barrier for users to engage with eGovernment services or b) because they impede supply, by acting as a disincentive or barrier for public sector organizations to provide eGovernment services.

We will try to identify the barriers of authentication and identification (in terms of disincentives or dampeners on eGovernment usage or supply) in terms of the four

[128] J. Dumortier and others, p. 12.

main characteristics identified in this definition: real or perceived and supply or demand.

5.1 Real supply side barriers

5.1.1 Brief description of the barrier: legislation delaying secure authentication

The availability of a secure authentication process is an important success factor for eGovernment [Cap Gemini/TNO 2004, p. 32]. An example of a secure authentication service is the digital signature, such as DigiD in the Netherlands. The use of different identity management systems in the Member States will certainly lead to interoperability problems at a European level.

5.1.2 The barrier and its implications (reasons why it is a barrier and the implications it may have for eGovernment progression both at regional, national and /or European level)

Laws or the legislation process with regard to secure authentication and privacy can delay the development of eGovernment [Cap Gemini/TNO 2004, p. 32]. Organizations have set up their own procedures instead of waiting for national standards for secure authentication. It seems that legislation is needed to create a pan-European standard for authentication and identification (identity management system). It has also been recommended in the Dumortier Report, that a more detailed study is necessary on the Internal Market consequences of the eGovernment programs of the Member States. The report warns that the “clear danger that these programmes will result in national barriers, fragmentation and interoperability” means support most be given to the interoperability between electronic signature applications at a European level. The reliability of digital identifiers (identity management) is of great importance for eGovernment services, and a government must be able to authenticate its citizens claims about their identities to fulfill its fundamental tasks.

5.1.3 Degree of severity

At a European level, eGovernment needs a secure and uniform identity management system, which could be met by drafting appropriate legislation at a European level to create a pan-European standard for a secure identity management system. The barrier therefore seems a surmountable hurdle e.g. with legal change (orange)

5.2 Perceived supply side barriers

5.2.1 Brief description of the barrier: uncertainty over identity management systems

Uncertainty about identity management systems might be a perceived barrier on the supply side. Governments and government agencies are not always certain about the legal acceptability of an identity system (like an electronic signature). Furthermore, the lack of interoperability of such identity systems could be a barrier. Although legislation exists at European level (Directive 1999/93/EC), the implementation of the directive throughout Europe should still be streamlined [Dumortier 2003, p. 13].

5.2.2 The barrier and its implications (reasons why it is a barrier and the implications it may have for eGovernment progression both at regional, national and /or European level;)

To overcome blockages create by this barrier, Directive 1999/93/EC should be re-interpreted and clarified [Dumortier, p 9]. However, at the same time it should be made clearer to national governments and government agencies which kind of identity systems can be used, for example whether a Qualified Electronic Signature should always be used or are alternative technologies also available?

The lack of interoperability has also been identified as a big obstacle for acceptance and the proliferation of electronic signatures [Dumortier 2003, p. 8]. As a result, many isolated systems of electronic signatures exist. It is clear that a lack of interoperability of identity management systems is a barrier for eGovernment services at a pan-European level. Therefore, it is important to promote interoperability of identity management systems (electronic signatures). It seems questionable whether this should be promoted by harmonizing legislative measures. However, one way or another, it seems important that the European Commission encourages the work on standardization of the technologies behind identity management systems, but at the same time it should leave space for alternative technologies to a standardized system, such as Qualified Electronic Signatures [Dumortier 2003, p. 13].

5.2.3 Degree of severity

The legal acceptability of different identity management systems should be clarified. It does not seem necessary to do this by drafting new legislations. The interoperability of national identity management systems should also be promoted at a European level. This seems possible by encouraging the standardization of technologies. It is not clear yet whether legal change or additional legal measures are necessary in this respect, or that the existing legal framework is sufficient. The barrier seems a surmountable hurdle (orange).

5.3 Real demand side barriers

5.3.1 Brief description of the barrier: identity theft

Identity theft refers to crimes and misdeeds perpetrated using the personal information of another [Camp, p. 10]. It involves the risk of losing one's digital identity through error, misuse or an identity abuse - such as identity theft or identity fraud - or the unauthorized access, modification, deletion or transmission of sensitive, high value or mission critical data and systems in commerce. It is a real barrier on the demand side, particularly for the end-user, e.g. affecting a consumer or citizen [NECCC 2002, p. 38].

5.3.2 The barrier and its implications

Identity theft is caused by weaknesses in identity management systems, combined with the increasing availability of personal information. It is estimated that annually between one quarter and three quarters of a million people in the US are victims of identity theft. A private research company even estimates that seven million

Americans were victims of identity theft in 2002. There is consensus that identity theft is a large and growing problem.

In the Netherlands, a Bill to introduce a general citizen service number (*Burger Service Nummer: BSN*) is currently being discussed in Parliament. The BSN would be used by every Dutch government agency from 2006. This would make it possible to combat fraud, but is also increases the citizens' vulnerability, as the more value that is added to a general identifier, the more will swindlers be interested in it. When government agencies have a blind faith in the citizens service number, they also will have too much trust in the false identity of a swindler.

It is quite a challenge for a citizen to prove his identity when his major identifying documents have been compromised. Information can linger in computers until manually removed, and many decisions are made by silently and automatically consulting databases. An individual may never know whether they have completely secured their identity. Technical and legal protection against identity theft is therefore important for gaining and keeping trust by the citizen in eGovernment.

5.3.3 Degree of severity

For misusing others' personal information, penalties have to be threatened and enforced for accountability mechanisms to work. Misuse can be malicious, by a government official or by a private party, but personal information can also be misused by mistake. Furthermore, individuals can act irresponsibly with their own data. One question is whether the legal system should pursue all kinds of disruptions of the security of an identity management system, including cases when an individual accidentally compromises the security of the system. To avoid such a legal issue, the identity management system itself should be made secure against the loss or abuse of data in identity management systems.

The question of whether legal changes are necessary, should be further researched. At least for pan-European eGovernment initiatives, harmonization of national legislation is necessary. This barrier also seems a surmountable hurdle (orange).

5.4 Perceived demand side barriers

5.4.1 Brief description of the barrier: users' uncertainty over identity management systems

A perceived barrier on the demand side might be the uncertainty of the citizen regarding the integrity and authenticity of an electronic signature (identity management system). Uncertainty about the reliability this system and about data sharing between governments can result in a lack of trust in online government.

5.4.2 The barrier and its implications

According to Camp [2003], trust is critical for any relationship, and therefore also for eGovernment. Trust also requires a reliable identity framework. An individual must be confident in the relevant attributes of other parties in any relationship. Confidence is also based on (good and reliable) reputations.

The importance of electronic identification and authentication is also stressed by the respondents on the survey recently published in Your Voice on eGovernment 2010.[129] According to 65% of the 232 respondents, the most important issue European eGovernment should focus on is “electronic identification and authentication”. Therefore, electronic identification and authentication is the most important key enabler for eGovernment. In addition, rather than preferring a single European scheme, most of the respondents think, that the use of the national electronic identification schemes should be enabled in transactions with other Member States. Consequently, most of the respondents think that the mutual recognition of electronic identities should be provided by Member States.

Lacking interoperability was considered as the main barrier in the area of electronic identification and authentication (58% of 150 respondents). The second most important barrier was (still) national legislation (51%). Other highly rated barriers are lack of awareness of benefits (43%) and lack of trust and security, whether perceived or real (also 43%).

Identity management may also be involve pseudonymous or even anonymous systems, but whichever approach is adopted if it manages all personal identifiers properly the system can improve trust in eGovernment. The Workshop on Digital Identity (Kennedy School of Government, April 28, 2002) called for policy shifts relating to identity management after exploring various future scenarios relating to identity theft, and loss of privacy. Such shifts include gaining greater awareness of the scope of the problems relating identity theft and (assumed) loss of privacy, including a better understanding of what identity management must, can and cannot do.

In this respect, individuals should be able to manage various existing identities of themselves involving various tokens and authorizations, such as nickname in some particular social contexts, a professional designation for work purposes and a stage name for their hobby rock band [NECCC 2001, p. 31]. It is also understandable that people want to separate their different identities by using different email addresses (for work and for private), business cards (for different employers) and other identity credentials for each name and corresponding realm of identity. At the same time, this may lead some people to create a personal file containing all the various usernames, passwords, system preferences, and other relevant information needed to keep grip on the identity systems in which a person participates. A number of years ago, it was proposed in the Netherlands that the citizen would use a “digital safe” for these purposes. However, a number of government agencies would also have access to this kind of personal and confidential information.

5.4.3 Degree of severity

At a European level, eGovernment needs to establish trust among citizens and other users in the integrity and authenticity of the identity management system that is employed. This should consider offering the possibility of pseudonymous or anonymous systems. Some for of legal protection against identity theft and protection of privacy should be sufficient to help address related problems. The barrier seems a surmountable hurdle (orange).

[129] Online Public Consultation; Report Jan 2006 V 1.0. Available on the Internet: http://europa.eu.int/idabc/servlets/Doc?id=24086

Intellectual Property Rights (IPR) and eGovernment
Dr. C Cuijpers and Dr. J. Nouwt, Tilburg Institute for Law, Technology, and Society (TILT), University of Tilburg, Netherlands

1. Description of the area

Many electronic services provided by governments relate to the dissemination of information. Governments can electronically disseminate information to their citizens as well as requiring citizens to provide information through an electronic medium. Intellectual Property Rights (IPR) could apply to this information exchange. These are rights given to people to protect their creative works. Other examples of what has been called 'informational goods' [Lodder and Kaspersen, 2002, p. 97] include: copyright and related rights; the protection of data bases; expert systems; (software) patents; trade secrets; trade names and trademarks; service marks; design rights; know-how; domain names; logos; and inventions.

Copyright and related rights play an important role in the information society as it stimulates creation and innovation. According to recital 2 of Directive 2001/29/EC: "copyrights and related rights protect and stimulate the development and marketing of new products and services and the creation and exploitation of their creative content".

Within eGovernment, use can be made of several creations of the minds of others. For example, governments can compile information themselves, or engage private third parties within this process. IPR can also be vested in the means of communication, such as the ICT infrastructure or the software, used by governments to communicate with, or deliver eGovernment services to, citizens or businesses.

2. Why could there be barriers to eGovernment in this area?

For governments, it is of great importance to assess the implications that intellectual property rights can have with regard to a specific form of electronic communications or a specific service delivery in order to avoid liability for a breach of IPR. When disseminating information, governments must pay attention to who owns the intellectual property regarding this information. When publications are made by private parties on the order of public authorities, a government agency needs to be sure that disseminating this information won't be in violation of the intellectual property of the private party. When governments request certain information to be delivered to them by private parties, the question also arises whether the private party can deliver this information to government without violating the rights of others who were responsible for creating the requested information.

To give a real life example: suppose that an archiving agency wants to digitize the complete collection of applications for building permits. This agency can make two violations of the law. First, the drawings within the building permits archives are copyright protected. In most cases, the originator of the drawings – often an architect – is the copyright owner. The storage of these drawings in a computer is an unauthorized reproduction, which can not be compared with copying information for educational purposes, or for private use by a natural person. Furthermore, the online distribution of information is also a way of making information available, which is not allowed, according to the EU's Copyright Directive (2001/29/EC).

In applying IPR to software, the following quotation is of interest: “The owner of intellectual property rights has the exclusive right to prohibit others from using those rights. Exclusive rights do not pose problems to the software ecosystem as long as the rights can be clearly separated from each other and the creators of new programs are not dependent upon the rights of others. Unfortunately, the implementation of even a simple computer program in the systems that are in use today typically depends on software components from many others. Thus, one company or independent developer can hardly produce a complete software product alone and without the explicit acceptance of others. Understandably, the fragmentation and overlapping of rights pose practical problems as software products become more complex and more parties participate in the development process. The interdependence of rights owners can create difficult lock-in situations if “difficult” rights owner tries to get as much control through the interfaces of exclusive rights. They may not license the intellectual property at all or may offer only non-acceptable terms. Especially open source developers seem to have a strict criterion that licenses cannot have any royalty requirements.” [1]

Another barrier that could originate out of intellectual property rights lies in the field of patent law. In theory, a patent on parts of a technology that act as gateways, and that therefore need to be interoperable, can be used to block access to new entrants, either by actually prohibiting access, but more likely by charging licensing fees that are too high.[2] In this respect, it might be necessary to establish a strengthened legal mechanism to force owners to open their technology to others if they are unreasonably restricting access.

In general, it is often stated that too strong intellectual property rights can lead to increasing costs, inefficient centralization, less innovation and, in the end, slower technological progress. All these issues can impede the development of eGovernment.

3. What is the European context for this area, including legislation, policy statements, institutional arrangements relevant to this topic?

Many regulations concerning IPR have already been proposed and implemented at the level of the European Community concerned with the establishment and functioning of the internal market.[4] The following topics have been covered in European directives: enforcement of intellectual property rights[5]; resale right for the benefit of the author of an original work of art[6]; copyrights and related rights[7];

---

[1] Välimäki, M., Software Interoperability and Intellectual Property Policy in Europe, *European Review of Political Technologies*, December 2005.
[2] See Harbour, M. and Gentry, S., Intellectual Property and the Challenge of Digital Technology, *European Review of Political Technologies*, December 2005.
[4] For an overview of the European directives relating to copyrights and neighbouring rights, see: http://europa.eu.int/comm/internal_market/copyright/index_en.htm
[5] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, *Official Journal* 30/4/2004, L 157, P. 0045 – 0086.
Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. *Official Journal* L 195 , 02/06/2004 P. 0016 – 0025.
[6] Directive 2001/84/EC of the European Parliament and of the Council of 27 December 2001 on the resale right for the benefit of the author of an original work of art. *Official Journal* 13/10/2001, L 272 P. 0032 – 0036.
[7] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. *Official Journal* L 167 , 22/06/2001 P. 0010 – 0019.

protection of data bases[8]; term of protection of copyright and related rights[9]; satellite and cable[10]; rental right[11]; protection of computer programs[12]; and semiconductors[13]. Legislation and proposed legislation concerning industrial property – including patents[14]; trade marks[15]; biotechnological inventions[16]; designs[17]; and the patentability of computer-implemented inventions[18] – can be found at the website of the European Union.[19]

Attention has been given to IPR not only at the European level, but also in a broader international perspective (e.g. WTO's TRIPS Agreement on Trade-Related Aspects of Intellectual Property Rights, see http://www.wto.org). TRIPS attempts to narrow the gaps in the way intellectual property rights are protected around the world, and to bring them under common international rules. The agreement lays down a minimum level of protection that each government has to give to the intellectual property of fellow WTO members. It covers: Copyright and related rights; Trademarks, including service marks; Geographical indications; Industrial designs; Patents; Layout-designs (topographies) of integrated circuits; Undisclosed information, including trade secrets. Other relevant international agreements include two coordinated by the by the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT) (see see http://www.wipo.int).

The large amount legal regulation in this areas does not guarantee that all IPR-related barriers to eGovernment have been lifted. There is much current academic discussion concerning the future of intellectual property and the need for flexibility within this system, as well in discussions on software patents and the threat to open

---

[8] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal* L 077 , 27/03/1996 P. 0020 – 0028.
[9] Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, *Official Journal* L 290 , 24/11/1993 P. 0009 – 0013.
[10] Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, *Official Journal* L 248 , 06/10/1993 P. 0015 – 0021.
[11] Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, *Official Journal* L 346 , 27/11/1992 P. 0061 – 0066.
[12] Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal* L 122 , 17/05/1991 P. 0042 – 0046.
[13] Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, *Official Journal* L 024 , 27/01/1987 P. 0036 – 0040. Official Journal L 024 , 27/01/1987 P. 0036 – 0040.
[14] The Directorate General for Internal Market and Services is at the time of writing (May 2006) consulting stakeholders on their needs in relation to the legal framework and possible actions in the field of industrial property. Views are sought on the patent system in Europe, and what changes if any are needed to improve innovation and competitiveness, growth and employment in the knowledge-based economy. The consultation focuses on three major issues: the Community patent; how the current patent system in Europe could be improved; and possible areas for harmonisation. The Commission is also seeking views on what action could be taken while work on the Community patent is continuing, in particular within the framework of the existing European patent system, or by bringing national patent systems more closely in line with each other through either approximation of laws or mutual recognition of national patents. The legal framework for jurisdiction over patent disputes is an area of significant interest in this context.
[15] See for the Commission and Council regulations in the field of Trade Mark Law http://europa.eu.int/comm/internal_market/indprop/tm/index_en.htm
[16] Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions, *Official Journal* L 213, 30/07/1998 P. 0013 - 0021
[17] Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs, *Official Journal* L 289 , 28/10/1998 P. 0028 - 0035
[18] The 6th of July 2005 the European Parliament has rejected the Councils' common position on patentability of Computer Implemented Inventions and the legislative procedure was closed
[19] http://europa.eu.int/comm/internal_market/indprop/index_en.htm

source software. Furthermore, questions regarding the level of harmonization also remain in areas in which Directives have been implemented. These concerns are illustrated here through the following comments on three Directives relating to: copyright; databases; and the re-use of Public Sector information.

The Copyright Directive (2001/29/EC) has been introduced as an essential building block for the Information Society.[20] The fourth recital of the Directive, the economic importance of harmonization of the European legal framework on copyright has been stressed:

> "A harmonised legal framework on copyright and related rights, through increased legal certainty and while providing for a high level of protection of intellectual property, will foster substantial investment in creativity and innovation, including network infrastructure, and lead in turn to growth and increased competitiveness of European industry, both in the area of content provision and information technology and more generally across a wide range of industrial and cultural sectors. This will safeguard employment and encourage new job creation."

However, a close reading of the Directive, can lead to the conclusion that the Directive does not really harmonize copyright law in the Member States. It leaves the Member States a large bandwidth within which to implement the Directive in their national legislation.

For example, Article 5 of the Directive leaves Member States the freedom to provide for exceptions or limitations to the rights provided for in Articles 2 (Reproduction right) and 3 (Right of communication to the public of works and right of making available to the public other subject-matter) for the "use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings."

As an explanation of this provision, recital 34 of Directive 2001/29/EC says:

> "Member States should be given the option of providing for certain exceptions or limitations for cases such as educational and scientific purposes, for the benefit of public institutions such as libraries and archives, for purposes of news reporting, for quotations, for use by people with disabilities, for public security uses and for uses in administrative and judicial proceedings."

This provision was new to some systems of law, but is also pertinent. In France, a litigant has been sentenced for counterfeiting for having read a text under copyright during a plea.[21]

---

[20] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. *Official Journal* L 167 , 22/06/2001 P. 0010 – 0019. Commission welcomes adoption of the Directive on copyright in the information society by the Council. Press Release, available on the Internet: http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/01/528&format=HTML&aged=1&language=EN&guiLanguage=en

[21] A.R. Lodder, H.W.K. Kaspersen, *e*Directives: Guide to European Union La won E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Socieity, and Data Protection. The Hague/London/New York: Kluwer Law International 2001, p. 109-110.

Information in databases is protected by national provisions based on the Database Directive (96/9/EC).[22] This harmonizes the copyright protection for databases. According to it, a 'database' means a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. Because the database protection is a *sui generis* protection, it differs from copyright protection in that it does not require any form of creativity from the originator. This also means that factual data can be protected on the condition that the data have been assembled in a database and that this activity has required a substantial investment. The contents of a database are protected if the process of obtaining, verifying and presenting the data elements represents a substantial investment in qualitative or quantitative terms.[23]

Even though the Database Directive seemed necessary to enact in 1996, its relevance is now being questioned, as is clear from a current evaluation of it.[24] Within this evaluation, four options are presented. One is to repeal the whole directive and another to repeal the *sui generis* right.[25] The evaluation invites stakeholders to provide further evidence on the economic impact of *sui generis* protection in stimulating the production of databases in Europe. It might be wise to reflect on the effect these options might have on existing or future eGovernment communications and services that make use of databases.

In the European context, it is also relevant to highlight what could be called the 'commercialization' of government information. This is regulated from November 2003 in the Directive (2003/98/EC) on the Re-use of Public Sector Information.[26]

Governments collect a lot of information for their administrative purposes. This is not only of importance for the participation of the citizen in a democratic society, but also has economic value. For example, government information is the raw material for the information industries to create value added goods and services, such as navigation systems or SMS-services for weather or traffic.

Member States are encouraged by the Directive, but not obliged, to make government information available for re-use for commercial and non-commercial purposes. An exception is made for documents that are copyright protected by third parties. This is explained in recital 22 of the Directive:

> "The intellectual property rights of third parties are not affected by this Directive. For the avoidance of doubt, the term 'intellectual property rights' refers to copyright and related rights only (including *sui generis* forms of protection). This Directive does not apply to documents covered by industrial property rights, such as patents, registered designs and trademarks. The Directive does not affect the existence or ownership of intellectual property rights of public sector bodies, nor does it limit the exercise of these rights in any way beyond the boundaries set by

[22] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. *Official Journal*, 27-03-1996, L 077.
[23] Schellekens, M. M. H. Intellectual Property Issues Relevant for the European Transport Information System. Giorgi, L., Klautzer, L., Rahman, A. and Schmidt, M. (eds.), *Towards a European Transport Policy Information System*. ETIS-LINK 2005, p. 142.
[24] http://europa.eu.int/comm/internal_market/copyright/docs/databases/evaluation_report_en.pdf
[25] http://europa.eu.int/comm/internal_market/smn/smn40/docs/database-dir_en.pdf
[26] 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*, 31-12-2003, L 345/90.

this Directive. The obligations imposed by this Directive should apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (the Berne Convention) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement). Public sector bodies should, however, exercise their copyright in a way that facilitates re-use."

Therefore, the Directive is not applicable to documents for which third parties hold intellectual property rights.[27] However, the Directive allows Member States to regulate that administrative bodies to make charges for the re-use of government information. The total income from supplying and allowing re-use of documents may not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment.[28]

Furthermore, it is left to the Member States to regulate that public sector bodies may impose conditions for the re-use of public sector information in a licence, dealing with relevant issues.[29] These relevant issues include: liability; the proper use of documents; guaranteeing non-alteration; and the acknowledgement of source. If public sector bodies license documents for re-use, the licence conditions should be fair and transparent. Standard licences that are available online may also play an important role in this respect. Therefore Member States should provide for the availability of standard licences.[30]

Although the Directive on the re-use of public sector information contributes to the transparency of activities by public sector bodies, it can be concluded that the Directive is not really harmonize the national provisions for such re-use. On several important issues, especially on the principles governing charging, a large bandwidth is left for the Member States.[31] For pan-European eGovernment, it is necessary to overcome these national differences, which might only be possible by imposing European standards, either in soft law, or in hard law.

4. What is the relationship of Intellectual Property Rights to the 7 barrier categories and associated research questions?

4.1 Leadership failures

Intellectual Property Rights seem to be of little importance for failures in political and management leadership. However, adequate leadership could result in attention being given to legal IPR aspects so it can be considered an element of management leadership that attention is paid to possible infringements of IPR. For instance, as is discussed later in this paper in Section 5.4.2, the municipality of Dordrecht (the Netherlands) warns users of government information of possible violations of intellectual property rights.

[27] Article 1(2)b Directive 2003/98/EC.
[28] Article 6 Directive 2003/98/EC.
[29] Article 8 Directive 2003/98/EC.
[30] Recital 17 Directive 2003/98/EC.
[31] K. Janssen, Hergebruik van overheidsinformatie – binnenkort ook bij u in de winkel? *Privacy & Informatie* 2006, 69.

4.2 Financial inhibitors

The costs of developing, implementing and maintaining ICT systems can be high. In this regard, intellectual property rights can also play an important role in areas we have already mentioned, like IPR for documents, the use of databases and software licenses. Therefore, IPR has financial consequences that could become a serious barrier to eGovernment. In this respect, an important question is how the costs of software licences are affecting investments in eGovernment? And are these costs leading to a greater use of free open source software[130]?

4.3 Digital divides

eGovernment resources can be used in different ways, for example depending on social and economic divides. From a social point of view, it can be supposed that the younger generation of consumers are less aware of IPR issues than the older generation and might be influenced by the fact that digital music and movies are freely available on the Internet. This might influence their (un) awareness of intellectual property rights.

From an economic point of view, eGovernment resources involving information that is protected by IPR (copyright, database protection, portrait right, etc.) could have their availability limited by their costs. In this respect, it is worth examining whether access to copyright protected information could be regulated by Digital Rights Management Systems. Furthermore, an agency could be blocked in attempting to digitize their archive of applications for building because the archive is copyright protected for the originator and so their storage on computers will be an unauthorized reproduction and the online distribution of such information will not be permitted under the Copyright Directive.

These are examples of possible IPR restrictions that could be of influence for this barrier. The main question that will be dealt with in this respect is therefore: Are there examples of IPR restrictions, including copyright, that are a barrier to eGovernment services?

4.4 Poor coordination

Coordination and harmonization are important issues for appropriate eGovernment networks and services. As we discussed above, the relevance of the Database Directive has been questioned in its evaluation. Furthermore, the Directive on the re-use of public sector information is not harmonizing effectively and seems to leave too much bandwidth for the Member States. With the Directive (1999/93/EC) on electronic signatures, there seems to be “a primary need for a consistent, clear and workable re-interpretation of the provisions of the Directive.”[131]

Therefore, the question seems relevant to find out if there are provisions in Directives that hinder the effectiveness of administration activity at different levels or

[130] See http://www.flossworld.org for information on the MODINIS initiative Free/Libre/Open Source Software.
[131] Dumortier, J. and others: *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, p. 9.

have become a barrier for the competitiveness of the European economy, and how they can be altered to remove the blockages?

4.5 Workplace and organizational inflexibility

The example at the start of the is paper of an agency archiving planning documents, such as in the case of the Dutch Digital Building Permit Office, shows that there is uncertainty about how to deal with database protection and architect copyrights covering drawings in the database. We also described above how in Dordrecht users of this information are warned that architect drawings are copyright protected. However, it can be assumed that not all similar projects inform their users about such legal issues. Dealing with such legal issues could become an administrative burden for public administration management and staff. They should therefore be well informed about these and other legal issues in order to be able to share their government information and documents in a legitimate way.

Because employment laws could inhibit flexibility in changing working practices or the deployment of staff, it is relevant to deal with the question of the ways in which the current structure of Employment Law in Member States act as a blockage or facilitator for the restructuring of the public sector labour market that may be needed to realize the full benefits of high levels of ePublic Services delivery and use.

4.6 Lack of trust

Trust is an important key element for the success of eGovernment. This means, for example, that citizens should not have a “Big Brother-fear” of government monitoring and intrusion in their lives and must be able rely on the security within eGovernment services. From an IPR-perspective, it seems important that citizens can rely on the legal compliance of governments with IPR when delivering their eGovernment services.

In this respect, it seems relevant from an IPR point of view to ask: “What have been the practical implications of the ways in which information in databases have (or have not) been protected by national provisions based on the Database Directive[132]”.

However, public administrations will also have to pay attention to other IPR-issues than database protection. for example, to prevent liability difficulties, and thus enhance trust, the information and documents that are available in eGovernment services should of course be in compliance with other intellectual property rights.

4.7 Poor technical design

eGovernment services will often be developed using certain specific or general software that is copyright protected. This could create difficulties regarding the use of such exclusive software rights, by means of licences or very inconvenient terms and conditions. On the one hand, using standard software can of course contribute to the standardization between eGovernment networks and services. On the other hand, using standard software can also have important technical (interoperability) and

[132] See Cuijpers, C. and Nouwt, J., ‘IPR and eGovernment’ regarding Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal of the European Union*, 27-03-1996, L 077.

financial consequences. Therefore, it is interesting to consider the use of open source software for eGovernment services, for example because open source software licences do not have royalty requirements.

In this respect, the way the open source movement is affecting interoperability is discussed below. For instance, is it constraining interoperability by offering only strict terms on licenses that do not have royalty requirements[133], which means other participants are not incentivized to comply with interoperability requirements. Or is it facilitating interoperability by removing problems caused by complex fragmentation and overlapping of IPR and copyright issues associated with individual software components of an eGovernment application?

5. What are the real and perceived barriers in this field?

This section reflects on barriers to eGovernment related to IPR in relation to the generic working definition of a barrier used for this project:: "Characteristics – either real or perceived - of legal, social, technological or institutional context which work against developing eGovernment at the EU level, either a) because they impede demand, by acting as a disincentive or barrier for users to engage with eGovernment services or b) because they impede supply, by acting as a disincentive or barrier for public sector organizations to provide eGovernment services."

5.1 Real supply side barriers

5.1.1 Brief description of the barrier: Copyright infringements

Private parties can contribute to eGovernment by generating publications and other information for it or by providing the ICT infrastructure or software needed to deliver certain electronic services. If the intellectual property rights relating to a publication, infrastructure or software are not transferred to the government, the use thereof by government can lead to IPR infringements. These can lead to another field of law, namely that of liability. So, if government makes use of private parties to create information or technological device to perform eGovernment services, government needs to be sure that disseminating this information or the use of these devices won't be in violation of the intellectual property of the private party.

5.1.2 The barrier and its implications

On the supply side, governments can take initiatives to make government information available for the public. We call this the 'active delivery' of public sector information. Publication of government information on a website represents a copyright-protected publication, for example according to Article 15b of the Dutch Copyright Act:

> "The further communication to the public or reproduction of a literary, scientific or artistic work communicated to the public by or on behalf of the public authorities shall not be deemed an infringement of the copyright in such a work, unless the copyright has been explicitly reserved, either in a general manner by law, decree or ordinance, or in a specific case by a notice on the work itself or at the

[133] Välimäki, M. (2005) 'Software Interoperability and Intellectual Property Policy in Europe', *European Review of Political Technologies*, December 2005.

communication to the public. Even if no such reservation has been made, the author shall retain the exclusive right to have it appear in the form of a collection his works which have been communicated to the public by or on behalf of the public authorities."[134]

This means that the information published by an administrative body can be used freely, unless the administrative body has made a reservation. To prevent third parties from using copyright-protected government information, the administrative body can make an explicit reservation. Furthermore, the administrative body could also make financial conditions for the further use of copyright-protected government information. For the active deliverance of the information, the administrative body needs the consent of the originator. When information is published without the originator's consent, and without the reservation mentioned above, the copyright of the originator has been released. The originator can no longer object to the further use of the information made available by the administrative body. However, he can claim compensation from the administrative body for violation of his copyright.[135]

A real legal barrier on the supply side exists when the originator of the information does not give his consent for publication of the information by the administrative body. To prevent this from happening, it might be necessary to adapt the Copyright Acts in the EU Member States. The adaptation of the European copyright law could, for example, create a legal basis for the publication of copyright-protected information by administrative bodies, or create an entitlement to financial compensation.

Another problem on the supply side can come into being with regard to authority over the eGovernment service. When government cooperates with private parties – in whatever legal structure – it is of eminent importance that government makes the appropriate agreements regarding emerging intellectual property rights. In this respect, mention can also be made of outsourced public sector services. Investment in such services is often to a large extent made by private parties as a way of assisting government achieve its public service objectives. However, if the private party owns the emerging intellectual property rights, the government's influence in developing and exploiting the eGovernment service might be limited and can lead to financial burdens. To minimize this risk, it might be best if the public sector is at least an equal investor in the IPR relating to, and emerging out of, eGovernment services.

5.1.3 The degree of severity of the barrier: *red*

European legislation should be adapted to help further harmonization of European copyright law, and to prevent legal barriers in cases when originators of information refuse to give their consent for publication of information by an administrative body. A general legal basis could be created for European governments to publish government information, or an entitlement to financial compensation for the copyright owner. Therefore, this barrier can be considered a serious concern that can only be overcome by a moderation of the European legislation (red).

---

[134] See http://www.ivir.nl/legislation/nl/copyrightact.html

[135] Bergfeld, J. P., Kaspersen, H. W. K. and Lodder, A. R., *Wob en ICT. Onderzoek naar de gevolgen van toepassing van Informatie- en Communicatietechnologie voor de Wet openbaarheid van bestuur*. Amsterdam, 2000. On the Internet: http://www.minbzk.nl/contents/pages/2134/evaluatie_wob_ict_11-00.pdf

5.2 Perceived supply side barriers

5.2.1 Brief description of the barrier: Open standards and open source software

An IPR barrier to eGovernment is the uncertainties within the European patent regime which pose a threat to open standards as well as open source software.

In the eEurope Action Plan 2005, the Commission stated: “an agreed interoperability framework to support the delivery of pan-European eGovernment services to citizens and enterprises” would be issued. It also states that the framework “will be based on open standards and encourage the use of open source software”.

Open standards are publicly available specifications that describe the characteristics of a technology with the aim of promoting technical interoperability.[136] Simply defined, this form of interoperability is the ability of two or more ICT assets (hardware devices, communications devices, or software components) to easily or automatically work together and to expand to include the ability of two or more business processes or services to easily or automatically work together. It is clear that this ability to interoperate is key to reducing ICT integration costs and inefficiencies, increasing business agility and enable the adoption of new and emerging technologies.[137] However, if the technologies to realize interoperability are patentable, and high fees are asked to use them, the positive effects of interoperability will certainly be reduced.

Open Source Software is software for which the underlying programming code is available to the users so that they may read it, make changes to it and build new versions of the software incorporating their changes. There are many types of Open Source Software, mainly differing in the licensing terms under which (altered) copies of the source code may (or must be) redistributed. Usually, a ‘perpetuity clause’ is used, stating that further improvements of the software will also be free (open source) software.

5.2.2 The barrier and its implications

The difference between a copyright claim regarding software and a patent claim is related to the scope of the protection. Copyrights rest only on the written programme (or code). A software patent relates to the invention and therefore is much broader. The European Parliament turned down a Software Patent Directive proposal in July 2005. Unfortunately, this means that the legal situation regarding the patentability of

[136] The EIF Working Document states that, in order to reach such interoperability in the context of pan-European eGovernment services, guidance needs to focus on so-called ‘open standards’. The latter term is defined in the EIF Working Document as a standard satisfying the following requirements:
the costs for the use of the standard: are low and are – the –the standard has been published; –not an obstacle to access to it; standard is adopted on the basis of an open decision-making procedure (consensus on the intellectual property rights to the standard, majority decision, etc.); are vested in a not-for-profit organization which operates on a completely free basis and there are no constraints on the re-use of the standard.
However this definition is criticized in literature. For example, Lueders , H., Intellectual Property Rights and eGovernment Interoperability in Europe, European Review of Political Technologies, December 2005 states: “When further defining ‘open standard’, the impact of any ‘open standard’ definition should be carefully assessed, taking into account the inherent interoperability logic. Moreover, when defining the term ‘open standard’, the EU should take into account the legal limits to any ‘open standard’ definition as delineated by public procurement and intellectual property law.”

[137] Lueders , H., Intellectual Property Rights and eGovernment Interoperability in Europe. *European Review of Political Technologies*, December 2005.

computer-implemented inventions remains unclear. The European Patent Office has granted thousands of software patents that may cover interoperability information. However, it is not clear whether those patents are truly valid.

To provide some legal certainty, and to prevent open standards and open source to be, it should at least be made clear: what can and what can't be patented; what exactly the definition is of interoperability; and if, how and when regulators can impose a requirement on a patent holder to grant a licence to open their technology to others.[138]

For the ICT industry at large, reasonably priced interoperability licence fees do not create barriers. However, many open source advocates, academics and some small companies argue that such standards essentially close interoperability information for those who cannot meet the licensing criteria in the licences.

The previously mentioned uncertainties regarding patentability and open source software are not the only bottlenecks that can be created by the use of open source software in eGovernment. As a survey in the Netherlands found:

> "Nevertheless, seventy percent of the interviewed government officials indicated that they thought the dependence on proprietary software companies to be too big. A survey of the use of open source software by educational institutions showed that open source software is being used, although the percentages are still low. Many educational institutions indicated that they needed more information about open source. The unfamiliarity with open source software is thus still a bottleneck. Sometimes the non-use of open source software by government can be traced back to trivialities. For instance, the requirements that the government sets for calls for tenders for software projects appear to discriminate against open source companies. Requirements of annual turnover and company size are set so high that many open source companies fall by the wayside. The Minister has promised to re-evaluate government policy with respect to tenders."[139]

The open source debate is also of relevance with regard to the development of eGovernment in poor nations. They won't be able to solve their development problems unless they stop having to pay high software licensing fees.

5.3 Real demand side barriers

5.3.1 Brief description of the barrier: legislation relating to standards and interoperability delaying secure authentication

An important real demand side barrier mention is blockages to the interoperability of technical systems used to provide eGovernment services. If only one computer system or only one type of computer software can be used to access eGovernment, citizens and businesses using different systems or software will simply be deprived of eGovernment.

[138] Article 31 of TRIPS already gives some guidance in this respect.
[139] Quotation from an interview held with Maurice Schellekens, an expert in national and international Intellectual Property Rights.

5.3.2 The barrier and its implications

eGovernment should not be based on one specific standard, technology or platform that obliges end users to apply this standard, technology or platform. As an example, the Dutch electronic tax form is available from 2006 only for the Apple and Linux platforms. However, enterprises and citizens should be able to choose between different suppliers of software that could help them to use the services of public authorities. Also, from the viewpoint of government this is essential with regard to the availability and cost-effectiveness of the service. A competitive strategy can ensure the presence of different products and lead to better and cheaper services. A condition that must be met for this to be achieved is that open standards are used and compatibility problems between different formats are solved.

The following quotation is illustrative of the related issues of whether only one or more technologies can be used, and the way that is closely related to discussions about the patentability of software:

> "Many technology companies would like to see their proprietary software technology become standard and then control the surrounding 'ecosystem'. To contrast, interoperable developers and the users of technology at large would like to see all standards to have open non-proprietary interfaces without any intellectual property protection. (...) European copyright laws have a well-established principle that a single right owner can't control interoperability information through copyright.[140] Unfortunately patent law does not know such exception: it must be therefore balanced through alternative means."[141]

The problems with regard to the uncertainties within the patent system have already explained in Section 5.2.1.

5.3.3 The degree of severity of the barrier: *orange*

From a legislative perspective, the barrier might be considered as a minor concern. However, it should be noted that European legislation could be a means to promote the interoperability by allowing the use of multiple open standards, technologies, or platforms. At the same time, legislation could be useful to clear uncertainties regarding the patent system. It is therefore a surmountable hurdle (*orange*).

5.4 Perceived demand side barriers

5.4.1 Brief description of the barrier: Copyright infringements

When government requests certain information to be delivered to them by private parties, the question arises whether the private party can deliver this information to government without violating the rights of others who were responsible for creating the requested information.

[140] Directive 91/250/EEC, Article 6.
[141] Välimäki, M., Software Interoperability and Intellectual Property Policy in Europe, *European Review of Political Technologies*, December 2005.

5.4.2 The barrier and its implications (reasons why it is a barrier and the implications it may have for eGovernment progression both at regional, national and /or European level)

A private party who delivers copyright protected information from another party to the government is liable for violating these copyrights. To apply for a building permit, citizens or other organizations often have to deliver drawings made by architects, which are copyright protected. This means that nobody is allowed to use these drawings for building purposes or distribute or copy them, unless consent has been given by the architect, who also has a copyright on drawings based on a client's clear instructions and ideas. The architect can transfer the copyright, for example under the condition that the drawings may not be changed or may be used only once. The architect can also ask for financial compensation.

It is questionable whether governments at national and European level can claim that they are not accountable for violating IPR in the same way as private parties. It should be investigated whether governments should have an obligation to notify the owner of a copyright before delivering his or her information to the government. Arrangements may have to be made with the receiving government, because the government could be obliged to make the information available to third parties.

In the case of passive, rather than active, delivery of public sector information, it does not seem justified for an administrative body to refuse a request based on a Freedom of Information (FOI) Act with a plea of their copyright. However, according for example to Dutch law, the receiver of the information does not have a right to free disposition of the information and needs the consent of the administrative body for copyright-related acts. It is questionable whether an administrative body is obliged to highlight such use limitations. Although the Dutch Copyright Act does not oblige the administrative body to do so, this seems to be a sensible thing to do.

In this respect, we can point at the Building Archives of the Dutch municipality of Dordrecht.[142] At the department of Building and Living (Bouwen en Wonen), an archive of data relating to homes and other buildings in the municipality is kept up to date. The archive contains building permits, demolition permits, building drawings, construction calculations, and construction drawings. Anyone can have access to this archive, and can take a copy of one or more of these archived documents, at reasonable costs. On the website of the Building Archives, some tips and points of interests are mentioned. One of these consists of a warning for copyright protected documents:

> "*In the archive, a lot of granted building permits are being retained. As is stated before, you can use these documents for example for your application. We urgently call for your attention that building drawings, construction drawings, and construction calculations are copyright protected. To make use of these documents, you need the consent of the copyright owner. You are responsible yourself for obtaining consent*."

[142] See: http://www.dordrecht.nl/pls/idad/prodEgemProductToon?F_PRODUCTID=999920021209131220

A warning like this can be considered an obligation for government, based on administrative carefulness. It is questionable whether leaving such a warning could be seen an unlawful act against the copyright owner.

5.4.3 The degree of severity of the barrier: *orange*

This barrier can be considered as a barrier of moderate concern. It doesn't seem necessary to change the legislation with regard to IPR, but there certainly are some legal points of interest. It should be noticed that a warning to the user of government information seems necessary from the perspective of fair administration. Therefore, the legal barrier can be overcome by taking other legal measures (orange).

Liability and eGovernment
Dr. C Cuijpers and Dr. J. Nouwt, Tilburg Institute for Law, Technology, and Society (TILT), University of Tilburg, Netherlands

1. Description of the Area

It is important to realize that eGovernment is not a one way street. Its purpose is not only to disseminate information from the administration to the public or to facilitate or enhance public services, but is also about information relationships between government, businesses and civilians. These relationships work both ways, in that two-way electronic access to basic administrative interactions, interactive communication and feedback on political initiatives are as important as one-to-many information and service delivery from a public body. An optimal functioning of eGovernment can therefore be described as involving four processes:

- information delivery;
- communication between public bodies and citizens/companies;
- transactions between the above partners;
- interaction and participation.

Within all these processes, there is a need for a division of responsibility regarding damages resulting from a malfunction in the process or from inaccuracies in the information being processed. This is what liability law is about: "Legal responsibility to another or to society, enforceable by civil remedy or criminal punishment".[143] The division of liability within eGovernment processes needs to be dealt with on the basis of general tort law and contracts, governed by general contract law. With regard to the contractual relationship, the law provides several mechanisms to deviate from the general rule that everybody is responsible for their own actions. Limitation and even exclusion of liability is possible, although only to a legally limited extent. The special role government plays within society can give reason to interpret very strictly the boundaries of limitations or exclusion of liability in the public sector, which raises the possibility of insuring liability risks.

2. Why could there be barriers to eGovernment in this area?

In electronic communications, all kinds of scenarios can be sketched regarding questions of liability. Messages or services can reach recipients too late, not at all or can be delivered to the wrong recipients. With regard to the contents, there can be inaccuracies or infringements of a law such as that relating to copyrights or privacy. These examples show that there is not always a distinct difference between electronic and non-electronic communication, in which the same errors can occur. However, in electronic communication the risks of a malfunction might be higher, the effect of the malfunction could lead to much greater damages and it might be harder to ascertain and prove where responsibility for the malfunction lies. This can, for example, be a result of information aggregation, in which process it might be hard to ascertain which source, or which combination of sources, lead to inaccuracies in the

[143] Blacks' law dictionary 2004.

information. Another problem can be the traceability of malignant third parties interfering in the eGovernment process.

Another reason for there being barriers to eGovernment within the field of liability is the different legal approach taken regarding contractual as well as non-contractual liability throughout the European Union. This point is of even greater importance with regard to electronic communications, as often the circle of parties involved in delivering the communication or the service is larger then in non-electronic communication. A simple example is communication by means of a letter, as opposed to the sending of an email. With the delivery of the letter, only government, the post company and the recipient are concerned. With the delivery of an email, the government probably needs to make use of an access provider, as well as a service provider. The same holds true for the recipient. The eGovernment process also involves software and hardware used by government and users to send and receive emails within which malfunction could also influence the electronic communication. This simple example shows that in electronic communication, and probably even more in electronic service delivery, the contractual relations might be more complex when using traditional means.

In relation to the content of information, there is not that much difference between electronic and non-electronic communication. A government official can as easily make errors in a letter as in an email. The question of whether or not it is easier for a third party to alter an electronic message or a traditionally written message is hard to answer in general, as it depends to a large extent on the security measures taken. In this respect, a direct link can be made to the contribution of the paper in this Part on Authentication and Identification. As already mentioned, the simple aggregation of information in an online environment could lead to a higher number of inaccuracies in the information being processed. On the other hand, ICT can easily be used to detect inaccuracies, to prevent inaccuracies from coming into being or to correct inaccuracies. To be able to come to a conclusion in this respect, empirical research is needed to ascertain whether or not, and under what circumstances, electronic information processing is more likely to generate inaccuracies than non-electronic information processing. The much greater ability to aggregate and integrate content and services from different organizations, in both the public and private sectors, can also lead to inaccuracies in the content through: a possible lack of visibility of the source of the problem; difficulty in proving causation; and the possibility of large scale damages in an electronic environment.

Another link that can be made is to privacy and data protection, as the aggregation and integration of information can lead to severe infringements resulting in liability risks. All these circumstances could inhibit moves to change from non-electronic to electronic means of communication and service delivery, as well as to the development of new electronic services. For instance, the introduction of a Dutch National Electronic Patient Record has been postponed because the gaining of unauthorized access by a hacker made it obvious that the level of security of the information within these records was not sufficient, which led to a perception among hospital managers of high liability that meant they naturally refused to take up this innovation.

In this respect, addressing eGovernment at pan-European level might increase liability risks as the complicated technical structure as well as the lack of uniformity

within the legal framework could cloud assessments of predictability and therefore makes liability assessment difficult.

3. What is the European context for this area?

Liability is an issue that needs to be addressed for all government actions. The risks for legal liability, resulting in financial responsibilities, need to be assessed for every form of interaction between government and citizens or businesses. As mentioned above, risks in an electronic environment can be different, especially with regard to the ease of crossborder activities within this environment. Government services are often confined to territorial borders, which simplifies and restricts the risks of liability. With pan-European eGovernment services, the crossing of borders is the whole idea, which leads to a much more complicated legal framework regarding liability.

In the EU there is no unified general law on contractual or non-contractual liability. Several projects are, or have been, run with the aim of harmonizing tort law, the law on contract and even on a 'European Civil Code'.[144] None of these projects has so far led to legally binding regulations.[145] However, it is possible to conceive of harmonized rules regarding liability issues within the Union. For example, several specific European directives contain clauses regarding liability in specific areas or concerning specific parties. The eCommerce Directive (2000/31/EC)[146] contains provisions regarding liability of intermediary service provides; Directives 1999/34/EC and 85/374/EEC[147] concerns product liability; the eSignature Directive (1999/93/EC) refers to national liability rules but does require a minimum level of liability[148]; and the unfair contract terms Directive 93/13/EEC[149] limits the validity of contract terms that exclude liability. Furthermore, in several fields of law in which directives have been adopted, there are provisions as to who will be liable for breaching the law under particular circumstances. Directives relating to database protection and privacy[150]

---

[144] Professor Dr. Dr.h.c. Christian von Bar and Professor Dr. Dr.h.c. mult. Ulrich Drobnig, Study on Property Law and Non-contractual Liability Law as they relate to Contract Law, http://europa.eu.int/comm/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/study.pdf

[145] Even though the Principles of European Contract Law (PECL) do not have the authority of national, supranational or international law, this does not mean they have no legal relevance. A choice of law for the Principles can be made in case of an international contractual relationship in order to overcome differences in national legislation. The choice for the PECL can be to avoid difficulties in agreeing on a national system of law. If no explicit choice of law is made in a contractual international relationship, the courts might apply the PECL. The justification for applying the Principles is that it is hoped that the they will furnish a more appropriate basis than any system of national contract law for the adjudication of an international contract (see D. Busch, Indirect Representation and the Lando Principles. An Analysis of Some Problem Areas from the Perspective of English Law, European Journal of Comparative Law, Vol. 2.3 December 1998).

[146] Directive 2000/31/EC of the European Parliament and of the Council 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 L 178, 17/07/2000 P. 0001 – 0015.

[147] Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Official Journal L 141 , 04/06/1999 P. 0020 – 0021. Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Official Journal L 210 , 07/08/1985 P. 0029 - 0033 (DA, DE, EL, EN, FR, IT, NL)

[148] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 13, 19/01/ 2000 P. 0012 -0020. Article 6.

[149] Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. Official Journal L 095, 21/04/1993 P. 0029 - 0034

[150] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, Official Journal L 077 , 27/03/1996 P. 0020 – 0028. 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 (Directive on privacy and electronic communications) Official Journal L 201 ,

are also of relevance in this respect. Even though these regulations bring some clarity to specific legal relationships, they do not constitute a harmonized legal framework regarding liability. Also the level of harmonization established by these directives is typically ambiguous, [151] as differences remain in interpretations of their provisions and in national legal implementations.

Without a European legal framework, liability for eGovernment is to a large extent therefore regulated by national law. Research undertaken on the harmonization of European law in this area has clearly revealed that within the European Union a legal 'rift' exists in liability law. For instance, many differences between contractual and non-contractual liability displaying a large variety of legal rules exist not only between Common Law countries (e.g. UK) and Civil Law countries (e.g. France, Germany)[152], but also between different Civil Law regimes. Research[153] regarding European Private Law seeking to answer the question of whether this rift should be solved by European legislative measures has so far indicated that the differences in the liability regimes lead to barriers to enter the European Market.[154] The arguments leading to this conclusion can also be used with regard to the question of whether the differences in liability regulations throughout the EU can be defined as a remaining barrier to eGovernment. These arguments are examined further in the next section.

4. The relationship of liability to the seven barrier categories and associated research questions

This section examines the relation of legal liability and the seven categories of barriers and associated research questions described in Part 1 of this deliverable. The financial inhibitors and lack of trust barrier categories are likely to be the most closely related with liability. However, poor coordination in relation to legislation is also tightly connected to liability. There is also a link with regard to workplace and organisational resistance and leadership failures. Digital divides and poor technical design do not seem to be that relevant, except if poor technical design is viewed

---

31/07/2002 P. 0037 – 0047. 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 L 281 , 23/11/1995 P. 0031 – 0050.

[151] For example, the evaluation of the e-Commerce directive shows a difference in scope of the articles concerning service provider liability. Spain and Portugal have In addition to the matters dealt with by Articles 12-14 decide to provide for limitations on the liability of providers of hyperlinks and search engines. First report from the Commission to the European Parliament, the Council and
the European Economic and Social Committee on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Brussels, 21.11.2003 COM(2003) 702 final.
http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2003/com2003_0702en01.pdf

[152] For this remark regarding tort law see: European Group on Tort Law, http://www.egtl.org/. For Contract Law see: Christian von Bar, Ole Lando and Stephen Swann, Communication on European Contract Law: Joint Response of the Commission on European Contract Law and the Study Group on a European Civil Code, European Review of Private Law 2: 183 –248, 2002.

[153] There are at least two groups doing research in this area. One is the European Group on Tort Law, which has published "Principles of European Tort Law, Text and Commentary. SpringerWienNewYork, 2005.
http://www.egtl.org

[154] For example: "Divergent contract law makes it at present impossible to engage effectively in the European market on an informed basis. Businesses which nonetheless dare to take that step are often burdened by costs which are either superfluous or unforeseeable. Risks of liability are extraordinarily difficult to gauge; often they are simply absorbed and may make business unprofitable or loss-making." von Bar, C., Lando, O. and Swann, S., Communication on European Contract Law: Joint Response of the Commission on European Contract Law and the Study Group on a European Civil Code, European Review of Private Law 2: 2002, p. 238.

from the perspective of liability for poor technical design. Liability for products and software used to establish a European infrastructure for eGovernment and to supply eGovernment services is, as shown in this paper, one of the factors to be taken into account in cost/benefit analyses regarding the development of eGovernment. In this respect, mention can also be made of possible liability for national authorities who do not comply with technical standards imposed by the EU or for other kinds of technical incompatibilities that should have been resolved. However, these liability issues can also be brought under the heading of financial inhibitors.

In Section 2 of this paper, several circumstances are described that could be a reason for a reluctance to change from non-electronic to electronic means of communication and service delivery, as well as to the development of new electronic services. This reluctance to initiate eGovernment can be an outcome of a cost/benefit analysis. The interpretation of such an analysis and its consequences is however closely related to workplace and organizational inflexibility as well as leadership failure (the fear of leadership failure might even lead to workplace and organizational inflexibility).

While poor coordination of the interpretation and implementation of European legislation and/or the lack thereof is an important barrier related to liability, poor coordination viewed from a more organizational perspective can also play a role in liability assessment as this requires cooperation between experts from different scientific disciplines and might involve several government institutions at different levels.

With regard to research questions associated with the barrier categories, Section 2 illustrated the need for research concerning the increase of liability risks that can be caused in the move from traditional public service delivery methods to electronic media. What are the relevant differences that bear influence on the liability risk? Furthermore, does the electronic environment and the novelty of the electronic service delivery complicate the assessment of risks? Does the assessment inevitably lead to the outcome that the risk for service delivery is higher in an electronic setting?

It is not only the technical features that influence the (possible) complexity of risk assessment or the (possible) increase regarding liability risks. The pan-European character of the eGovernment services might complicate the allocation of legal responsibilities or the assessment of these responsibilities. As mentioned before, crossborder activity leads to difficult questions in identifying applicable law and competent forums, as no unified legal framework regarding liability exists in the EU.

In short: Does an ICT-based eGovernment environment create a higher risk of liability then is the case with the same kind of service delivery in a traditional (non electronic) environment? Do pan-European eGovernment services increase liability risks caused by the lack of a unified European legal framework regarding contractual and non-contractual liability? If so, does this mean that harmonization of legislation is a necessary precondition of the development of eGovernment?

Another question that needs to be taken into account concerns already harmonized fields of liability law. As mentioned before, even though directives harmonizing certain liability aspects do bring some clarity, the achieved level of harmonization is

often ambiguous as there remain differences in interpretation of the provisions of the directive, as well as differences in national implementation law. An evaluation of the practical impact of the liability clauses in the Directives concerning product liability (e.g. for eCommerce, eSignatures and unfair contract terms) should give an insight into the influence these regulatory initiatives have had on the development of eGovernment. This evaluation can provide relevant information with regard to the more general question regarding the necessity of harmonization of liability law at a European level in order to evolve eGovernment at this level.

5. What are the real and perceived barriers remaining in this field?

This section addresses the generic working definition of a barrier used for this project: “Real or perceived attributes of legal, social, technological or institutional contexts that constrain the development of eGovernment at national or regional levels. Such constraints can arise 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.” In this respect, a real barrier is a situation where there needs to be a change in the law in order for eGovernment to progress. Before exploring the real and perceived barriers remaining in the field of liability, it might be helpful to make a division between liability itself, and liability law.

The question as to whether liability is or can become a barrier to developing eGovernment largely concerns the financial risks that might be a disincentive for public sector organizations when considering the provision of eGovernment services. In this respect, not only is it necessary to assess the risk of malfunction, but so is an assessment into the damages that can be caused, the likelihood of being able to trace the wrongdoer and proof of causation. What it comes down to is a cost/benefit analysis that can become a financial inhibitor.

One of the main problems regarding a cost/benefit analysis in relation to eGovernment services can be the lack of predictability. New technologies for which no experience yet exists make it difficult to foresee possible failures or success rates. This lack of predictability may in itself lead to a perception of high risks regarding the development of eGovernment.

There are a number of scenarios relating to reactions to a perceived high risk related to liability for the malfunction within an eGovernment process. For example, government may decide not to make the changeover from non-electronic to electronic means of communications or service delivery, or to refrain from developing a new kind of electronic service. In this respect, the fear of liability and its consequential financial burdens can form a strong blockage to eGovernment developments.

Another reaction could be that government decides to use limitation and exclusion of liability to lower the risk. Possibilities for insuring the liability risks could also be taken into consideration. However, the insurer will rely on a similar kind of cost/benefit analysis to that undertaken by government. Thus, if the risks of a certain electronic service delivery are not yet clear, insurance might not be offered or only at an extremely high premium.

To avoid the risk of liability, and the potential associated financial burdens, government could also choose to divert liability to other parties involved in the eGovernment process. In this respect, two problems arise. Businesses that government need to involve in the development of eGovernment will themselves use extended exclusions of liability. It is general practice, especially in automation contracts, to exclude indirect damages completely.[155] Secondly, government could decide to revert liability to the users of its eGovernment service, which can lead to barriers on the demand side as fear for liability and lack of trust on the demand side can impede eGovernment.[156] And lack of trust can be seen as one of the key barriers to eGovernment. The correlation between liability and trust can be very significant in this respect.

The question as to whether liability law impedes eGovernment is hard to answer in general. Even though the outcome of the research in the field of European Private Law points to the necessity of harmonizing European liability law, this does not mean that every eGovernment initiative is hampered by a lack of harmonisation. For example, purely national initiatives will in principle not be affected by differences in national liability laws. However, pan-European initiatives in which many different parties from a lot of different Member States participate may not be pursuable because of the high, or unclear, risks for liability resulting from the differences in national liability laws.

For instance, a study of European Contract Law[157] outlines the difficulties in confronting businesses and consumers in ascertaining foreign private law and the economic ramifications of legal diversity for the EU internal market. The various European contract laws on non-performance or defective performance are based at present on fundamentally different regimes: either a system of strict liability or a system of fault-based liability. Just as substantial are the differences in the law on validity of penalty clauses and limitation of actions. Disclaimers can be mentioned as an example of uncertainty in this respect, even within national borders. For example, in the Netherlands the status of disclaimers is still unclear. The Dutch Information Office concerned with eGovernment services states in its legal Frequently Asked Questions that disclaimers cannot be used by government because of its duty of care and the General Principles of Good Administration. Moreover, as verbal promises can already be binding upon government, the same holds true for an email.

It is obvious that different views in respect of the value of such disclaimers leads to great legal uncertainty, not only with regard to government but also in general, as private parties can be involved in eGovernment. In turn, legal uncertainty is a barrier to eGovernment as liability risks are unclear. This can lead to a lack of trust in the eGovernment service and, therefore, reluctance to switch from traditional to electronic means of service delivery in terms of both the demand and supply sides of eGovernment.

---

[155] For information on Automation contracts, see Berkvens, J. M. A., van Esch, & van Geest (Eds.), Automatiseringscontracten, modellen voor de praktijk (losbladig) (pp. 1-52). Deventer: Kluwer.

[156] If the government finds it necessary to limit or exclude liability to a high degree, this can be interpreted by the end users as the eGovernment service not being trustworthy. This is a very relevant issue as studies show the public's use of eGovernment to be particularly low. Dutton, W.H., Di Gennarco, C., and Hargrave, A.M. (2005), The Internet in Britain, available at http://www.oii.ox.ac.uk/research/oxis/oxis2005_report.pdf

[157] von Bar, C., Lando, O. and Swann, S., Communication on European Contract Law: Joint Response of the Commission on European Contract Law and the Study Group on a European Civil Code, European Review of Private Law 2: 2002, P. 183 and 238.

In this research regarding European Contract Law, it has also been concluded that neither the mechanism of choice of law nor the freedom to frame contracts enables parties to avoid substantial costs which arising out of the real or supposed diversity of the law in the EU. Already the anxiety that differences in other legal systems might result in different legal outcomes leads to a considerable expenditure or effort to obtain very specific legal information and opinion, which in the end may turn out to have been unnecessary. Mention is made of the unnecessarily high premiums for liability insurance because of the very different liability regimes with regard to cabotage transport, an area that is even already dominated by international conventions.[158] Even though these research results cannot support the conclusion that in general harmonization of liability law is essential to avoid impeding eGovernment, they do not mean that an ongoing effort to harmonize contractual and non-contractual liability would in general be beneficial to the development of not only eGovernment but also eCommerce. In this respect the recommendation of Von Bar and Lando to carry out further work in formulating Principles of European Patrimonial Law, both for the sake of 'soft law' and as a pre-requisite for possible future legislation, is specifically interesting to pursue with regard to eGovernment.[159]

As described above, liability law as such is not in itself a real barrier to eGovernment. Liability law is merely a mechanism to allocate legal responsibilities as a means of removing blockages to eGovernment progress . These responsibilities can, in specific situations depending on many variables in particular contexts, lead to great financial risks on both eGovernment supply and demand sides. Thus, each and every eGovernment initiative requires its own a cost/benefit analysis as the basis of which a decision should be drawn as to whether to proceed with the initiative or to await certain kind of adaptations, legal or otherwise, to reduce the liability risks. Even if this analysis shows that it might not be wise to proceed with the eGovernment initiative under the present conditions, the initiating government is still free to decide that the risk is acceptable in the circumstances. This need to assess liability risks specifically for each and every eGovernment service further indicates why liability is not in general a real barrier.

The foregoing shows it can be difficulty to make a clear division between real and perceived barriers when discussing liability law. The following sections therefore address only perceived eGovernment supply and demand side barriers as this enables many the sketching of illustrative cases in which the diversity in legal liability regimes or the risk of being liable could in some circumstance not form a barrier to eGovernment. For example, this is the case when the liability risks regarding electronic communications or service delivery are no higher then in case of non-electronic communications or service delivery. However, as mentioned above, adopting more principles like the Principles of European Contract Law would create more legal certainty and increase the situations in which liability law, and the fear of being liable, do not form a barrier to eGovernment.

[158] Communication on European Contract Law: Joint Response of the Commission on European Contract Law and the Study Group on a European Civil Code, European Review of Private Law 2: 183 –248, 2002. P. 183, 197, 202 and 203.
[159] Idem, P. 183.

5.1 Perceived supply side barriers

5.1.1 Brief description of the barriers

This paper has already identified key perceived barriers to eGovernment relating to liability. Therefore, this section gives a general resume. The perceived barriers highlighted indicated that they can exist in two main supply-side situations:

a) If the risks of a malfunction are higher in electronic communications and service delivery then they are with traditional means of communication or service delivery, a blockage to eGovernment progress is likely to exist when:

   - in an electronic environment legal relationships are likely to be more complex;
   - in an electronic environment the visibility and predictability of risks might be more complicated;
   - Ii an electronic environment it can be more difficult to determine who the wrongdoer is;
   - in a electronic environment it might be harder to trace malignant third parties that have interfered in the communication or service delivery;
   - in an electronic environment it might be harder to proof the relation between conduct and damage; and
   - in an electronic environment the effect of malfunction within the eGovernment process, as well as inaccuracies within the content, can lead to much greater damages.

b) If there is substantial fear/uncertainty/anxiety regarding legal liability due to differences in national liability law and the lack of harmonisation in this field.

As described in Section 5.4, liability issues mainly relate to the key barriers of financial inhibitors and lack of trust. On the one hand, liability can lead to severe financial burdens on the demand side as well as the supply side, depending on the applicable legal and contractual framework. Too high a financial risk, or at an operational level the risk of non-performance or incorrect performance of service, leads to a lack of trust to use the service or to deliver the service. Therefore, the division of liabilities bears influence on trust. Exclusion of liability on the supply side might give a demand side perception that the service may not being trustworthy. On the other hand, if a supplier is so confident with regard to its service that it accepts all liability, this might boost confidence on the demand side.

5.1.2 The barrier, its implications and degree of severity

What has already been aid about cost/benefit analysis and liability is relevant to the first bullet point in the previous subsection. Such analysis should answer the question as to whether the eGovernment service is exposed to higher liability risks than the same service offered by government by non electronic-means. Important

aspects to be taken into account have been listed. Some of these aspects can be coped with by amending legislation, but most of them relate in one way or another to security measures, particularly their technical and organisational dimensions. However, the outcome of a cost/benefit analysis is can lead to answers to questions about whether or not a barrier to the initiated eGovernment process exists, whether or not this has implications on the (further) development of this process or the severity of this barrier that could have a detrimental impact on an eGovernment initiative. Also, the question as to whether legislative or other measures need to be taken to lift the barrier should flow from this analysis. With regard to the technological turbulence, cost/benefit analyses should be undertaken regularly to support the system's sustainability.

With regard to the second bullet point, it is already been stated that the development of soft law mechanisms to harmonize liability law is, in general, a necessary step towards further development of eGovernment. In this respect, some issues need special attention:

- Clarify the status of different legal provisions to limit or exclude liability, such as the legal status of disclaimers, general terms and conditions such as penalty clauses and limitation of actions, copyright notices and trade mark notifiers.

- Clarify whether or not the special position government has in society leads to the conclusion that government cannot, or to a lesser extent, limit or exclude liability.

- Provide principles to be used as a choice of law in order to overcome national differences in liability law.[160]

5.2 Perceived demand side barriers

5.2.1 Brief description of the barriers

The main barrier on the demand side related to liability arises when it leads to such a substantial lack of trust in eGovernment services among citizens and businesses that they will not use eGovernment facilities unless obliged to do so by government. However, lack of trust does not relate only to liability risks. Even if government is completely liable for the malfunction of the electronic communication or service, and there is no liability on the user, the citizen might still want to use traditional means of communication or service delivery if they are of the opinion that this is safer or easier. Even if not held liable, it can be very burdensome if a communication or service malfunctions. Thus, trust does not relate only to government, but also to the technique used by government.

[160] Research regarding European Contract Law has concluded that neither the mechanism of choice of law, nor the freedom to frame contracts, enables parties to avoid substantial costs which arise out of the real or supposed diversity of the law in the EU. Communication on European Contract Law: Joint Response of the Commission on European Contract Law and the Study Group on a European Civil Code, European Review of Private Law 2: 183 –248, 2002. P. 238.

5.2.2 The barrier, its implications and the degree of severity

As mentioned above, the involvement of citizens and businesses in eGovernment processes is a very important issue with regard to the development and flourishing of these processes. eGovernment is something that must be driven by the wishes of the public, not be based on government imposition. On the other hand, if interested parties are not troubled by the absence of eGovernment provisions, then there won't be pressure on government from the demand side to introduce such services. In this respect, a link can be made to the key barrier of workplace and organizational inflexibility.

In order to promote a more positive view of eGovernment among its citizens, efficiency advantages seem to play only a minor role. The absence of liability risks, trust in the functioning of the system and the ease to use the system[161] are much more important issues. Certainty regarding the legal framework, as well as limiting government possibilities to revert liability to the users of eGovernment, might increase trust to some extent. However, advice and education in relation to citizen could be of greater importance. For business user of eGovernment, on the other hand, efficiency and cost reduction are important factors. Legal certainty and the minimization of costs, in order to ascertain liability risks as well as for actually being liable, are therefore a high priority to business users eGovernment.

5.3 Conclusion

An important component in developing eGovernment lies in managing legal risks. This involves identifying and analysing potential risks and developing plans on how to control and monitor these risks, and how to respond to them. With regard to eGovernment at a pan-European level, tools to assess legal risks should be developed.

Amending and harmonizing existing legislation can contribute to the development of eGovernment. It has been recommended that the establishment of liability principles at a European level to overcome national differences in liability law should be pursued. However, in order to lift all remaining barriers, a complementary approach is required. In addition, it is also important to create trust in eGovernment among end users and to implement an adequate infrastructure – or at least interoperability of existing structures – and appropriate electronic communications and service delivery, involving private/public partnerships when appropriate.

[161] Anne-Marie Jorritsma, a former Minister in the Netherlands and currently mayor of a Dutch Local Authority, refers to the expectation that electronic government services are complicated, as being one of the main reasons for citizens not to use eGovernment services. Nederlandse Zaken, wake up call voor de digitale overheid, Magazine Bestuursacademie Nederland.

Privacy and Data Protection in eGovernment
Cristina Dos Santos and Professor Cécile De Terwangne, CRID, University of Namur, Belgium

1. Description of the area

Privacy and the protection of personal data are fundamental rights, which ensue from Article 8 of the European Convention on Human Rights: the right to private and family life, home and correspondence. These rights are now included in a wide range of legislation at European and Member State levels, as well as in Articles 7 and 8 of the European Charter of Fundamental Rights proclaimed in Nice on 7 December 2000[162].

Data protection is related to the protection of personal data, which means any information relating to an identified or identifiable person ('data subject')[163]. Data protection rules do not, in principle, prohibit the use of personal data but they offer a legal framework to allow data processing – provided specific requirements are met and special rights are granted to data subjects. The major principles encompassed by such rules are: respect of the purposes of data processing announced at the time of data collection; proportionality (balance between the interest of processing data and the data subjects' interests); and transparency.

The independent EU Advisory Body on Data Protection and Privacy, the Data Protection Working Party, has produced a document[164] on the protection of individuals with regard to the processing of personal data. This emphasized that data protection issues are involved in the development of various types of eGovernment projects and therefore needs careful consideration to ensure the success of these initiatives. Important related issues include the institution of a unique entry point to online administrative services, the institution of unique identifiers – such as personal identification numbers (PINs) – or even the implementation of interconnections between public databases.

2. Why could there be barriers to eGovernment in this area?

Data protection legislation is certainly a barrier to eGovernment in the sense that the protection of personal data rules can prevent or constrain some relevant activities, such as the processing of information about individuals (and in some countries also of information about legal persons[165]) or the transfer of data to other public bodies and other entities.

The implications of such legislation extend to all eGovernment areas as data protection rules affect: access to public documents containing personal data; the sharing of such documents between different entities; and the re-use of such

[162] These are incorporated in the draft Treaty establishing a Constitution for Europe as Part II.
[163] See Directive 95/46/CE, Article 2(a): "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity", i.e. the 'data subject'
[164] Data Protection Working Party (2003), *Working Document on E-Government*, Adopted on 8 May 2003 (10593/02/EN – WP 73)
[165] As in Italy, for instance.

documents. These rules could therefore hinder the development of businesses offering information services or information products incorporating personal data, including for instance the liability of the controller who determines the purposes and means of processing the personal data.

The contributions of delegations from various European Member States to the Data Protection Working Party (2003) document also highlighted the diversity of the questions dealt with by European Data Protection Authorities in relation to the general framework of eGovernment development. This diversity and the solutions developed to address different contexts, which may sometimes be very different or even conflicting, can be significant blockages to the development of a harmonized European legal framework.

Moreover, the existence of a range of too many actors at all levels (international and European, national, regional and local) without a common "data protection culture" or shared guidelines could be also a factor of "bad governance"[166], because the different interpretations and actions given by different actors could create substantial and disruptive tensions between stakeholders and in the way services operate in different arenas.

At the European level, Regulation (EC) 45/2001 of the European Parliament (2001)[167] established the European Data Protection Supervisor (EDPS) to monitor[168] the application of this Regulation's provisions in relation to all processing operations carried out by a Community institution or body (except the Court of Justice acting in its judicial capacity). Each Community institution (or body) also needs to appoint at least one person as Data Protection Officer (DPO), who must respond to and cooperate with the EDPS[169]. Many efforts are being made by the EDPS to develop a network with these DPOs, under the supervision of the EDPS, to ensure effective compliance with Regulation (EC) 45/2001[170].

The EDPS and the DPOs recognize not only that all EU bodies needed to appoint a DPO, but that this appointment does not in itself imply automatic compliance with the regulation[171]. The EDPS therefore emphasizes that DPOs must be notified adequately of personal data processing within their institution or body (in order to notify the EDPS, where appropriate, of any processing operations that entail specific risks for the people concerned and which therefore need to be checked by the EDPS beforehand). This is a problem concerning the transparency of data processing for EU institutions and bodies, and of public administrations more generally.

There are also difficulties of shared competences and liability where many stakeholders share networked resources. In such circumstances, when data is mishandling or errors are created, for instance by uncertainties related to managerial and operational responsibilities in providing content to eGovernment services, it

[166] See the comments of the European Data Protection Supervisor (2005), Second Annual Report 2005.
[167] This Regulation covers the protection of individuals with regard to the processing of personal data by the Community institutions and bodies as well as the free movement of such data.
[168] The regulation specifies the main duties of the EDPS as covering "supervision", "consultation" and "cooperation". See www.edps.eu.int for more information on the EDPS.
[169] See the provisions of the Article 1, 24 and following of the Regulation (EC) 45/2001.
[170] This is a main objective for 2006 specified by the EDPS in his Annual report for 2005.
[171] See DPOs' paper 'Profile of DPO and good practice manual' and EDPS' paper 'Position paper on the role of data protection officers in ensuring effective compliance with Regulation (EC) N° 45/2001'.

could be very difficult to assign responsibility to a particular entity because there is no general guidelines about assigning such responsibility.

Despite these potential problems, the protection of personal data could be compatible with the development of eGovernment applications, provided an appropriate balance is maintained between the efficiency of administration and the protection of individuals' data. From this perspective, the solutions adopted at the European level regarding European public documents and the protection of the privacy and personal data in those documents could be of great assistance to eGovernment initiatives[172].

3. What is the European context for this area, including legislation, policy statements and institutional arrangements relevant to this topic?

The right of protection of personal data ensues first from different international legislations. For instance, it is consistent with the approach of the European Court and the European Commission of Human Rights "who regard the [Convention] as a living document which evolves so as to meet new problems[173]". These bodies have come to regard data protection as a right falling within the scope of Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which provides for a right to respect for private and family life, home and correspondence, subject to restrictions being allowed only under certain conditions. The European Convention on Human Rights also protects the right to information (Article 10).

Both these fundamental rights had to be reconciled to given them the same protection level beyond national borders. The Council of Europe therefore drew up the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[174] in 1981, also known as 'The Data Protection Convention' or 'Convention 108'. This convention remains the unique legal binding tool at the international level, with universal application and open to all countries, even those who are not a member of the Council of Europe[175]. Some countries have drawn up national data protection laws according to the principles set out by this convention, such as the Irish Data Protection Act of 13 July 1988.

Subsequently, at the European Union level, the protection of personal data was enshrined in a larger legal framework, such as Article 6 of the EU Treaty and Article 286 of the EC Treaty[176], which reflects work undertaken by the EU and the Council of Europe over a longer period. This right has been mainly harmonized at European level by two Directives, as implemented by Member States: 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; and Directive 97/66/EC,

[172] See the 'Opinion 7/2003 on the re-use of public sector information and the protection of personal data' adopted by the Art. 29 - Data Protection Working Party on 12 December 2003.
[173] See: http://www.coe.int
[174] This Data Protection Convention was drawn up within the Council of Europe and opened for signature by the Member States of the Council of Europe on 28 January 1981 in Strasbourg (ETS N° 108).
[175] 35 Member States of the Council of Europe, including all EU Member States, have now ratified it.
[176] Adopted in 1997 as part of the Treaty of Amsterdam, this Article requires that Community acts on the protection of individuals with regard to the processing of personal data and free movement of such data should also apply to Community institutions and bodies, including the establishment of an independent supervisory authority.

concerning data protection in the telecommunications sector, which has been replaced by Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications.

Directive 95/46/EC is based on the principles of Convention 108, but has specified and developed them in many ways. It aims to provide a high level of protection and a free flow of personal data in the EU, so laid down a general framework for data protection law in Member States. It has also established a number of "protection institutional bodies" to control and monitor the appropriate application of the Directive. These bodies include:

- national supervisory authorities (e.g. the Commission for the Protection of Privacy in Belgium; CNIL in France; the Danish Data Protection Agency; and the 'Garante' in Italy);

- Article 29 of the Data Protection Working Party (2003), which has been implemented by Article 29 of Directive 95/46/EC[177]; and

- a Committee to assist the European Commission on issues related to data protection[178].

There is also Regulation (EC) 45/2001 of the European Parliament, which deals with general principles like: fair and lawful processing by Community institutions and bodies of personal data; proportionality and compatible use of such data; special categories of sensitive data; information to be given to the data subject; and the rights of the data subject and their supervision, enforcement and remedies.

The rules referred to in Article 286 of the EC Treaty have been laid down in this Regulation[179], which also established the EDPS as an independent supervisory authority at the European level[180]. Moreover, the Treaty establishing a Constitution for Europe, signed in October 2004, places great emphasis on the protection of fundamental rights, including the protection of personal data. The *Annual Report 2005* of the EDPS concludes that "this clearly indicates that data protection is now regarded as a basic ingredient of good governance" and emphasizes that "an independent supervision is an essential element of this protection".

Despite this European harmonization, there are important disparities at the Member States level regarding the implementation of Directives related to data protection. A significant one addressed in this paper concerns the inclusion or exclusion in the protected data of data regarding legal persons. Furthermore, European legislation relating to data protection brought some constraints regarding the development of eGovernment: access, use or any other processing of personal data are indeed limited to specified purposes and can be further processed only in ways compatible with those purposes.

[177] The relevant tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC.
[178] Implemented by Article 31 of the 95/46/EU Directive.
[179] Until the adoption of Article 286 of the EC Treaty, there was no legal basis for the Community institutions and bodies equivalent to the legal safeguards of the Directive 95/46/EC, which enabled them to take part in a free flow of personal data and subject with equivalent rules of protection.
[180] Its tasks and powers are described in Articles 41, 46 and 47 of the Regulation.

For instance, the Directives require that t Member States shall determine the conditions under which a national identification number or any other identifier or general application may be processed. These are key issues for eGovernment applications that aim at developing generalized internal use or cross-border transfer of such personal data.

4. What is the relationship of Privacy and Data Protection to the seven barrier categories and associated research questions?

Privacy and Data Protection legal issues are relevant to all seven barrier categories.

5. What are the real and perceived barriers remaining in this field?

Here the discussion will focus on two aspects:

1. How the lack of harmonization of data protection regulations at different levels can bar access to information from certain stakeholders (e.g. because of prohibitions on data sharing or data processing incompatible with the purpose of collection of these data; or through restrictions of access to personal data). These issues are identified as supply side barriers in Section 5.1.

2. How the lack of trust in eGovernment services and confidence in their security and privacy safeguards and controls can hold back stakeholders from using some or all eGovernment services because of a fear of an intrusive 'Big Brother' State or concerns about the inappropriate 'secondary use' of personal information in computer databases. Other related potential obstacles to eGovernment include worries about the lack of transparency of certain personal data processing mechanisms and which countries are suitable for engagement in cross-border information flows containing personal data. These aspects are examined in Section 5.2 on demand side barriers.

5.1. Supply side barriers

5.1.1. Networked administration and data protection rules

The traditional structure of public administrations was based on a 'silo model', in which each organizational unit within a vertical hierarchy has well-defined competences, with its own information at its disposal to achieve its duties and with its own way of processing that information. This framework has therefore resulted in vertical and closed information systems specific to each hierarchical unit.

In such a silo model, communication of information between public bodies were rare and severely regulated. Sharing information with external organizations (e.g. at a different level of administration, a foreign authority or a private-sector organization) was even more restricted. This vertical framework was seen until the late 20th century as a safeguard for citizens against the power of an omniscient State.

With the development of eGovernment, the silo model has shifted to a 'network model' of governance, with functional units linked by digital networks. This enables

public administrations to communicate internally and externally quickly and efficiently across institutional, political and geographic boundaries.

Although from the viewpoint of technological innovation such a networked governance models may be seen as positive progress in itself, the way this could remove the traditional guarantee against 'Big Brother' must be carefully and fully considered to ensure it does not lead to obstacles to eGovernment. For example, data protection regulations could bar access to stored information from certain stakeholders, and they can also prevent the sharing or communication of such data.

Although efficiency, for example of processing data, is an important value to promote inside a public administration, the quantity and sensitive nature of personal data processed by public bodies and the compulsory character of its collection indicate that other values must also be considered as important priorities.

This point is closely related to the difficulties in reshaping organizational structures and processes for a shift to networked governance processes[181].

5.1.1.1. A problem of access to stored data: avoiding repetitive requests for the same data:

By implementing eGovernment, Member States tend to organize the functioning of their public administrations so as to avoid repetitive requests for the same data to a citizen or enterprise. This implies the sharing of information among the interested bodies.

One must favour the technical solution that leaves responsibility for the data with the public authority that first collected it and allows other authorities to access the data, instead of creating a new commonly shared database gathering all the data collected by different authorities.[182] In that case, effective interoperability could provide the right answer from the data protection point of view.[183]

Another type of solution was chose by the Belgian Walloon Region[184]. In its ' eGovernment and Readability 2005-2009 Plan', it opted for the principle of a unique collection of the personal data of its citizens. This would enable every administrative service to find quickly the necessary information nearby the 'authentic source' (which held the information from the beginning), often by means of a direct communication from application to application, and each research will keep a track of the moving party to guarantee the transparency of the processing to the personal data subject (and this track will be visible when the person concerned accesses his/her personal file).

Another crucial issue is the regulation of access to data, which requires determining who may access what data (and who holds this data). This can be facilitated by implementing the 'purpose principle'[185]: a public body may have access to data only if that is necessary to complete its duties and legal obligations. Moreover, the public

[181] See the first barrier mentioned above.
[182] See the example of the Belgian "Social Security Crossroad Bank".
[183] See Section 5.1.2 on dealing with interoperability.
[184] For this Action Plan in its entirety, see: www.wallonie.be and http://easi.wallonie.be
[185] Stated in Article. 6, 1. (b) of the Directive 95/46/EC.

body may access only the data that are adequate, relevant and not excessive in relation to the purpose for which they are accessed[186]. And citizens must be informed of any shared access to their data[187].

This kind of solution should not be seen as the independent outcome of a particular individual body (such as a Region or a local administrative agency), but should be regarded as being subject to national guidelines and/or even something like a European 'code of conduct'. Such a framework should seek to guarantee aspects like: equality between the users at all organizational levels; transparency of personal data processing; and the effective interoperability between administrations.

In its 2004 Annual Report, the EDPS commented that even Community institutions and bodies were affected by this problem regarding the relationship between public access to documents and data protection. To address this, the EDPS, announced the development of a policy paper[188] on how to promote public access to documents together with the protection of personal data. According to EDPS, this may entail a clash between two fundamental rights: the right of public access to public documents[189] on the one hand, and the right to privacy and data protection[190] on the other. In this paper, the EDPS maintains that there should not "be a hierarchical order – and often no tension - between both rights, but as the objective of the first was to foster access to all documents, whereas the second must guarantee the protection of personal data, a tension could arise in some cases". The paper concludes that these rights must be seen as complementing – rather than competing with – each other.

This paper by the EDPS also aimed to give practical guidance to EU institutions and/or bodies in cases where there is a need to establish whether a document that contains personal data should be disclosed to a third person. According to Article 4(1)(b) of Regulation (EC) 1049/2001, the right to public access could be limited by a number of exceptions as it relates to privacy and data protection. However, it imposes three conditions, all of which have to be fulfilled for an exception to public access to apply:

1. "Privacy of the data subject must be at stake" (but there must be a qualified interest of a person involved).

2. "Public access must substantially affect the data subject" (and there must be a degree of factual harm to his or her privacy, because the public – intended as the users or as the public institutions – should not be deprived of their right to access if the privacy of the data subject would be only superficially affected by disclosure.)

3. "Public access is not allowed by the data protection legislation" (here the principle of the right to information, with the principle of proportionality playing a key role).

[186] Article. 6, 1. (c) of the Directive 95/46/EC.
[187] Articles 10 and 11 of the Directive 95/46/EC.
[188] See the EDPS' Paper about "Public access to documents and data protection" (July 2005), where he has issued guidelines for dealing with requests for access to public documents containing personal data.
[189] Laid down in the Regulation (EC) 1049/2001 (hereafter: 'Public Access Regulation').
[190] Stated by the Regulation (EC) 45/2001 (hereafter: 'Data Protection Regulation').

Finally, the EDPS recommended that "EU institutions and bodies must conduct a concrete and individual examination of each case … because compliance with both rights can be enhanced by proactive work, informing the data subjects properly in advance of how personal data will be dealt with – in full respect for the relevant Regulations"[191].

5.1.1.2. A problem of sharing data: the unique entry point to online administrative services and newly oriented services:

Unique entry points to online administrative services are being established[192] , which means data protection requirements must be respected when there is a reorganization of the 'back office' administrative systems that do not interface directly with citizens and businesses but which are linked to the development of such unique entry points. All information converges to the unique entry point, be it on entry or when being used. Here, more than ever, the principle of transparency in all steps of the processing must be followed by public bodies in order to guarantee the respect of all legal conditions of Directive 95/46/CE.

Public administrations that have been developing new services oriented toward 'life-events'[193] (e.g. a giving birth or changing job) or business-episodes[194] (e.g. employing staff or acquiring a business licence) need to gather information held by different administrative bodies. For example, a family intending to change locality could, if they so desired, have their aggregated data profile analysed by local public administration bodies. Based on this analysis, they could be informed of educational and health facilities, housing entitlements, job opportunities, etc., specific to their family circumstances. While the response might come from multiple agencies, the family would initiate a single 'life event' transaction, and would not have to re-supply to each agency involved information already provided to another public body. The response from public administration agencies would be based on authorized access to aggregate data on the family, and not on individual responses to agency-specific sub-sets.[195]

To set up and offer to citizens and enterprises such services, Member States need to able to link and combine content from multiple and diverse information resources, as well as making sure that all data sharing is managed in a safe way according to data protection principles.

---

[191] Here, and in its Annual Report 2005, the EDPS also suggested that persons concerned should be given the ability to opt out from disclosure on compelling and legitimate grounds.

[192] See, for instance, the CRID's report about the implementation of an unique entry point per Belgian borough (with a XML data sharing) in "Standardisation d'un guichet digital et échange de données en XML" (October 2002).

[193] The term 'life events' refers to the government services needed at specific stages in life. Typical examples of life events include: having a baby; starting/leaving school; changing employment status; being a victim of crime; moving home; becoming disabled; retiring; dealing with bereavement. (European Commission (IDA) 2004, *Linking up Europe: The importance of Interoperability for eGovernment Services*, Commission Staff Working paper, IDA publications, January 2004, available at, http://europa.eu.int/idabc/en/document/2036/5583

[194] The term 'business episodes' refers to the components of the business life cycle. Typical examples of business episodes include starting a business, employing staff, acquiring a licence, statutory returns, taxation, closing/selling a business. (European Commission (IDA) 2004). An example of *e*Government services based on business episodes at the national level can be found in the Irish Government's 'Basis - Business Access to State Information and Services' (http://www.basis.ie).

[195] Example cited in European Commission, "Linking up Europe: the importance of Interoperability for eGovernment services", Commission Staff Working paper, IDA publications, January 2004, available at http://europa.eu.int/idabc/en/document/2036/5583

For instance, in the Belgium case mentioned above, it was recommended[196] that public bodies should set up a 'digital track' to guarantee in an efficient way the security and the transparency of such processes, i.e. when a public body benefits from a right to access to the personal data of a natural person, this transfer would establish a digital track about which the person concerned would have knowledge. The same kind of track would be created for all data processing using the personal data of citizens, which would be available to the person to emphasize the transparency of such operations. In this way, the 'digitization' of data flows would permit a better 'trail' of the personal data processing. The EDPS proposed has proposed such a trail for e-monitoring of traffic and for budgetary purposes (including the verification of authorized use)[197.]

5.1.1.3. A problem of communicating data: self-administration

In some Member States[198], taxation services have adopted a new policy concerning income tax. In this approach, forms are pre-filled by the tax authority before being sent to the concerned person, which has only to check the registered amounts and sign the form. To realize this, the taxation services have to ask several different services to communicate the necessary data. Here too, data protection rules apply, for example requiring the taxpayer to be informed that data collected by another service is being communicated to the taxation authority. This must also respect the relevant conditions of Directive 46/95.

5.1.2. Interoperability and data protection rules

According to the European Commission (IDABC) (2004), "Interoperability means the ability of information and communication technology (ICT) systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge."[199] This is typical of the way EC official documents treat interoperability not only in terms of the use and interlinking of large scale information systems, but also with regard to the technical, organizational and semantic[200] opportunities they open to access or exchange data, or even of sharing or merging databases[201]. The European Data Protection Supervisor has underlined that this is regrettable "since different kinds of interoperability require different safeguards and conditions"[202].

Data protection does not create any problems in the examples highlighted by the Commission [203] in the areas of cross-border company registration, interoperability in

[196] By the CRID team in a Report for the "SSTC-Privacy" Project in October 2002.
[197] See the paper by the EDPS on Electronic Communications (2006).
[198] In France and Norway, for example.
[199] *European Interoperability Framework for pan-European eGovernment Services*, version 1.0, November 2004, http://europa.eu.int/idabc/en/document/3473/5585.
[200] Communication from the Commission to the Council and the European Parliament, *Interoperability for Pan-European eGovernment Services*, COM (2006) 45 final, 13 February 2006
[201] See also Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, 24 November 2005, http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0597en01.pdf .
[202] European Data Protection Supervisor, *Comments on the Communication of the Commission on Interoperability of European Databases*, 10 March 2006, available at www.edps.eu.int.
[203] Communication from the Commission to the Council and the European Parliament, *Interoperability for Pan-European eGovernment Services*, COM(2006) 45 final, 13 February 2006.

European eProcurement or in the need to reduce the administrative burden on enterprises in the EU through more effective and efficient interoperability[204]. However, concerns about data protection legislation are naturally raised as soon as interoperability is seen as a means of serving the exchange, gathering or sharing of personal data ("any information relating to an identified or identifiable natural person"[205]).

The Commission is conscious of the data protection issues linked to interoperability. It has emphasized that "Pan-European e-Government services need to ensure uniform levels of personal data protection… Full compliance with the existing European and national data protection legislation should be ensured. When available, technologies that are privacy-compliant and privacy-enhancing should be used".[206]

In certain documents, however, the Commission focuses mainly on technical and organizational aspects of the concept of interoperability. This has led the EDPS to declare officially[207] that he does not share the view that "interoperability is a technical rather than a legal or political concept". He added:

> "Indeed, it is obvious that making access to or exchange of data technically feasible becomes, in many cases, a powerful drive for de facto acceding or exchanging these data. One can safely assume that technical means will be used, once they are made available; in other words, it is sometimes the means that justify the end and not the other way around. This can lead to subsequent demands for less stringent legal requirements to facilitate the use of these databases: legal changes quite often confirm practices which are already in place." [208]

This remark seems to be compatible with the Communication from the Commission to the Council and the European Parliament on Interoperability for Pan-European eGovernment Services, issued at about the same time as this comment from the EDPS: "Technologies and market products are evolving. While new ways of ensuring interoperability are emerging, the increasing potential to enrich eGovernment services means that interoperability is becoming an issue where previously it was not."[209]

Previously, the Commission had stated:

> "Interoperability of databases is a key requirement for the development of new added-value services and for cross-border government information services. Furthermore, the interoperability of databases and the information they contain would allow public administration to implement 'value added' client-centric

[204] Except in Member States where information relating to legal persons is protected under the national data protection legislation the same way as information relating to natural persons.
[205] Article 2(a) of the 95/46/EU Directive.
[206] See European Commission, European Interoperability Framework for pan-European eGovernment Services», version 1.0, November 2004, http://europa.eu.int/idabc/en/document/3473/5585.
[207] European Data protection Supervisor, Comments on the Communication of the Commission on interoperability of European databases, 10 March 2006, available at www.edps.eu.int.
[208] ibid.
[209] Communication from the Commission to the Council and the European Parliament, Interoperability for Pan-European eGovernment Services, COM (2006) 45 final, 13 February 2006.

services that cannot be implemented on disaggregated information. These would typically involve the provision of client-specific services that can only be determined when client data from multiple sources is aggregated and evaluated as a whole".

This indicate indicates the need to be conscious at all times of raise important data protection and privacy issues when sharing and exchanging information.

5.1.2.1. Interoperability to facilitate the exchange of information v. data protection rules regarding the communication of data

When the concept of interoperability is used as a platform to facilitate the exchange of information, the question of the lawfulness of that communication of data needs to be addressed. In some such circumstances, data protection rules could restrict the communication of personal data. As the EDPS has emphasized, even when eGovernment developments do not lead to the creation of new databases they necessarily introduce a new use of existing databases by providing new possibilities for accessing them databases. The EDPS sees this as one of the main reasons why the concept of interoperability has to be examined very carefully.

5.1.2.2. Interoperability to allow the pursuit of new objectives v. the purpose limitation principle

Large scale ICT systems allow the pursuit of new objectives that go beyond the original purpose of the data processing objectives of that system. This automatically requires a new and complete analysis of the impact of the current system on the protection of personal data. In this context, the EDPS stresses that the interoperability of systems must be implemented with due respect for data protection principles and, in particular, the 'purpose limitation principle', which the Commission has explained in the context of interoperability as indicating that measures need to be taken "in which individuals have the right to choose whether their data may be used for purposes other than those for which they originally supplied the data in question."[210,211]

5.1.2.3. Interoperability and data protection rules on data quality

Rules relating to data quality do not generally impede exchanges of information, but do require that data are communicated only if they are adequate, relevant and not excessive in relation to the purpose for which they are collected and further processed.

5.1.2.4. Interoperability and the right to correct data

Data subjects are granted the right to obtain, as appropriate, the rectification, erasure or blocking of data whose processing would not comply with the provisions of Directive 95/46, in particular because of the incomplete or inaccurate nature of the data. The organization of the information system managing and processing the data

[210] The European Court of Justice has emphasised in its judgement of 20 May 2003 in the Rechnungshof case the importance of the cumulative application of articles 6 and 7 of Directive 95/46/EC.
[211] See European Commission, *European Interoperability Framework for pan-European eGovernment Services*, version 1.0, November 2004, http://europa.eu.int/idabc/en/document/3473/5585

must guarantee that a request for rectification of data signalled to an organization is transmitted to all connected organizations that have previously accessed the inaccurate data (e.g. in transborder taxation activities).

5.1.2.5. Interoperability and the duty to inform data subjects

The increasing of flows of personal data within and between public administrations and their citizens and businesses, including across national borders, has increased the importance of respecting the duty to provide data subjects with appropriate information regarding data processing activities being undertaken on information about that subject, as well as of changes to those activities[212].

5.1.3. The introduction and the use of PINs:

The growing use of ICT has led public administrations to have more recourse to identifiers, such as the Personal Identification Number, which could encroach upon personal privacy, especially when they can be used to interconnect different files relating to the person identified. It is necessary for countries, and the EU overall, to careful evaluate the costs of using PINs (e.g. in terms of data protection and privacy problems) and their benefits (e.g. increased administrative efficiency and lower economic costs).

Even if no specific reference to PINs is made in international human rights instruments, a number of international treaties are of particular relevance to the use of PINs, such as the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data alludes to them. The European Commission of Human Rights has on at least three occasions been confronted with issues relating to the use of PINs by public administrations: *Lindquist against Sweden* (N° 10879/84); *Lundvall against Sweden* (N° 10473/83); and *Kolzer against Sweden* (N° 11762/85).

As the basic principles laid down in the Data Protection Convention are intimately linked to personal data processing, they can undoubtedly help to control the use made of PINs as the key to personal data files. As the Committee of experts on data protection found in its 1991's study[213], PINs fall within the definition of personal data set out in Article 2.a of the Data Protection Convention, which implies that the following legal barriers must be considered by public administrations:

- The data user should obtain a PIN from an individual, company or organization fairly and lawfully in accordance with the requirements of Article 5.a of the Convention: there must be a statutory requirement of lawful authority to enable a PIN to be requested from its holder. In the absence of such a justification, the individual's free and informed consent should be sought before it may be collected.

- The same principle applies to the purpose for which a PIN is initially envisaged, in that it should not be used in a way or for purposes that were not contemplated originally (Article 5.b).

[212] See, for example, reports from the EDPS and for the European Ombudsman published on April 2006.
[213] See: Council of Europe, *The Introduction and Use of Personal Identification Numbers: The Data Protection issues*, Study of the Committee of experts on data protection (CJ-PD), Strasbourg 1991.

- PIN should not be composed of too much personal data, given the purpose for which it is to be used (Article 5.c).

- PINs should be accurate and reflect changes in the circumstances of the bearer (Article 5.d)

- PINs should not be composed in such a way as to reveal the categories of sensitive data referred to in Article 6 of the Convention.

- PINs should be kept secure against unauthorized access or dissemination to third parties (Article 7 of the Convention);

- The holder of a PIN should be able to exercise rights of access, rectification and erasure with regard to the data contained on a coded PIN, as well as to the personal data files to which the PIN relates (Article 8).

These conditions could become legal obstacles to eGovernment at the international level, but can also be considered as facilitators if they increase trust among users by providing legal minimum safeguards and offering transparency for file interconnections. This would be achieved by maintaining an appropriate balance between privacy requirements and the potential advantages of PINs for public administrations (e.g. in terms of administrative efficiency; more uniform and manageable methods for identifying persons other than through their names; cost savings; and rapid accurate identification and monitoring).

For instance, a PIN originally created as a number issued for the social security context could quickly become an all-purpose standard number/identifier[214]. However, this does not guarantee the data protection of the individual concerned. The relationship between data protection and the introduction and use of PINs are also confirmed by the specific reference to them in certain national data protection laws, such as:

- In France, Section 18 of the law of 6 January 1978 states that the use of the national index identification number with a view to personal data processing may only be authorized by order of the *Conseil d'Etat* after an opinion from the CNIL[215] (the French data protection authority). The CNIL has built up an extensive case law on the interpretation of Section 18 and has sought to restrict the interpretation of the meaning of the word 'use'.

- In Denmark, data protection legislation governing private registers requires that PINs may be stored by private bodies only if this is authorized by law or if the individual has consented, and provided it is necessary for the body holding the PIN to possess the information to satisfy legitimate requirements.

Even in the absence of a specific reference to the competence of data protection authorities to intervene on occasions when the use of PINs raises data protection problems, some national authorities have shown their willingness to police their use.

[214] As noted by the drafters of the Recommendation N° R (86) 1 of the Committee of Ministers of the Council of Europe on the protection of personal data used for social security purposes (Principle 5).

[215] "Commission nationale de l'informatique et des libertés".

For example, the Swedish Data Inspection asserted its competence when authorities seek to match files with the aid of PINs because the Swedish Data Act stipulates that it is necessary to have the approval of the Data Inspection Board before matching can take place. In accordance with Section 6, §1 of this Act, the Data Inspection Board may prescribe how the PIN should be used or it may prohibit the use of the PIN altogether. The same goes for the use of PINs in customer files, for instance the Data Inspection Board is competent to forbid the registration if the disclosure of the PIN of an individual can be considered as an unreasonable condition.

Furthermore, the laws which usher PINs into society may contain specific safeguards regarding their use, as well as for the individuals or bodies competent to use PINs. This is the experience of countries with legislation governing population registers (e.g. Denmark, Norway, the Netherlands, Belgium) or which have introduced specific PINs in specific contexts (e.g. Portugal, Switzerland).

There is also no doubt that PINs, in conjunction with automatic data processing, tend to increase the power of the public administrations, for instance as file interconnection via the use of unique identifiers allows administrative bodies to match up personal information held in various distinct files in a way that excludes the data subject from the information circuit. Moreover, a PIN may not be confined to public sector uses, but also to the private sector.

Such assessments of PINs in terms of 'power' raise questions about individual freedoms and control, since the citizen's anonymity is reduced by the existence of an identification number that may stay with the person for life. This makes it easier for the authorities to trace the whereabouts, movements, etc of citizens and to compile information from different personal data files without their knowledge and then to take decisions on the basis of this accumulated information.

There are differences between Member States legislations about whether or not to use a unique identifier or multi-standard number (e.g. Sweden, Denmark, the Netherlands, Belgium) or context-specific PINs in several areas of the public administration (e.g. Austria, Cyprus, France, Germany, Ireland). these could become obstacles to a uniform, or at least harmonized, European legal framework and can be considered as perceived supply side barriers in terms of perceived risks for the individuals.

5.2. Demand side barriers

5.2.1. Lack of trust

The main barrier on the demand side is the lack of trust in eGovernment services and confidence in their security and privacy safeguards and controls[216]. A wide European web-based survey[217] regarding eGovernment services has sought to answer the question: 'What do users really want from online public services?'. This gathered important data from ten European countries on a wide range of topics, including: access to technologies; the use of the Internet and other ICT-enabled

[216] See the fifth barrier mentioned above.
[217] See the "eUSER population survey 2005" on the IST-sponsored eUser Project at http://istresults.cordis.europa.eu/index.cfm?section=news&tpl=article&ID=81713) realised in 10 EU Member States, and the project website http://www.euser-eu.org

services; the attitudes of end users towards technology in general and the Internet in particular; and users interaction with providers of services of public interest in the areas of health, education and public administration. The eUser project is supporting wider policy and research activities in the EU to help better address user needs in the design and delivery of eGovernment services.

Among other things, this survey has identified users' fears about supplying personal information online (expressed by 45%) as an "anticipated barriers to eGovernment before use"[218]. Although there are some important differences between countries, there was no distinction between older and newer Member States. For example, fears about supplying personal information online were much higher than average in the UK, Ireland and Hungary.

These 'anticipated barriers' were generally also much higher than the barriers experienced once eGovernment was used. Once citizens have used eGovernment services, the barriers appeared less – though still important – and were related mainly to the difficulty of feelings of being left alone without sufficient support to assist in solving problems or questions[219]. In fact, fewer users have experienced barriers or difficulties (between 17% and 32%) compared with the number of users who perceived barriers before use (between 25% and 58%).

An interesting point[220] is that when citizens need to identify themselves when using eGovernment services, most have used simple, well-know methods such as a user ID and password or PIN codes. these are considered by experts as the simplest, cheapest and least secure methods, and not always suitable for legal or financial transactions. Therefore, user identification still remains a barrier to online communication and to services involving transaction, although there is also evidence indicating that more sophisticated methods , such as digital signatures or smart cards, are often rated as being as easy to use as the more well-known methods when they have been provided.

The eUser survey also demonstrates that there are important differences between countries. Italy, for instance, is leading on the use of user ID/password and PIN codes, compared to Poland which has the lowest use of these. Indeed, two of the four New Member States surveyed (Poland and the Czech Republic) did not show the pattern typical of the eight other countries, in which user ID/password and PIN codes are by far the most common methods. The data seem to indicate that in these two countries at least, some focus and investment has been made on more 'advanced' methods, particularly the use of specialized smart cards. In terms of the most advanced methods, Slovenia and Denmark led on the use of digital signatures and the Czech Republic on the use of specialized smart cards. The very high use of credit cards in Ireland is probably related to the fact that some revenue-raising transaction services (such as motor tax) are now fully available online.

[218] See http://www.euser-eu.org/eUSER_PopulationSurveyStatistics.asp?KeyWordID=1&CaseTitleID=838 (Chart 10)
[219] See Chart 11 of the survey.
[220] See "Authentication and Identification" in the survey.

5.2.2. Problems with data security

The main fear about the security and amount of data communicated to public bodies through electronic medium is that it will be accessed by unauthorized persons, communicated to unauthorized persons or lost because of a technical problem. The more sensitive the data is, the more acute is the fear.

Public Administration Transparency and eGovernment
Professor Cécile de Terwangne, CRID, University of Namur, Belgium

1. Description of the area

Public administration transparency relates to the availability to the public of public sector information and the transparency of democratic processes (e.g. the holding of open meetings or open online forums). Freedom of Information (FOI) legislation relating to public administration transparency plays a significant role in the development of eGovernment services, especially regarding the obligations of 'active transparency' requirements for information to be made publicly available by public authorities. Most Freedom of Information Acts are adopted at national (or even regional) level, which brings severe divergences between the Member States. Problematic issues in this regard are, for instance, the differences concerning exceptions existing in those regulations such as allowances for public authorities to refuse access to certain public documents (e.g. in case of conflict with data protection rules or national security confidentiality needs). The way those exceptions should be interpreted still needs to be clarified at European level. The only European harmonization that has taken place to date – justified by the principle of subsidiarity – deals with environmental public documents and transparency for public procurement.

2. Why could there be barriers to eGovernment in this area?

Public administration transparency can be categorized under 'e-services' and 'e-democracy'. As transparency is an expression of eGovernment, barriers to transparency represent barriers to eGovernment. Barriers can be found in the lists of exceptions to transparency foreseen in FOI Acts, in the lack of public awareness of the availability of loads of information, in the difficulties in locating information because of insufficient meta-data maps to guide seekers in the right direction, in the lack of access to appropriate technological tools or in the lack of individual skills to use the electronic media. Traditional FOI Acts are mainly focused on passive transparency and push only marginally the active dissemination of public sector information. This characteristics of FOI national legislation is not a barrier as such, but shows the limits of such Acts in providing an incentive to the development of information services through the Internet.

Transparency also means access to national information in order to process it and, possibly, to offer pan-European eGovernment services. In this context, even where transparency exists because access to public sector information is granted, some barriers can remain to an overall European transparency and to the offer of pan-European services based on this information (e.g. the problem of different languages or restrictions on re-use of received data).

3. What is the European context for this area, including relevant legislation, policy statements, institutional arrangements relevant to this topic?

A particularity regarding access to public sector information in the EU is that there exists no harmonized regime at EU level for this.[221]

[221] Please note, however, that most of the regimes are based on the content of Resolution R(81) 19 of the Council of Europe. The access regimes are hence not completely different to each other.

Each country organizes its FOI Acts according to its own administrative regulation and practice. All Member States have traditionally had some form of administrative secrecy for many centuries.[222] After important struggles for increased openness, Member States have increasingly adopted Freedom of Information Acts introducing laws and regulations concerning the right of access to the information held by public bodies. All these Acts also contain some exemptions to the guaranteed right of access.[223]

Currently, European FOI-related legal regime are limited to the following categories of information and issues:

- freedom of access to environmental information;
- access to information on public procurement; and
- the re-use of public sector information.

In the environment domain, the need for harmonization resulted in the adoption of the international Convention of Aarhus (UN/ECE Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters)[224] signed by the European Community on 25 June 1998, and two European Directives (90/313 of 7 June 1990 on the freedom of access to information on the environment and 2003/4 of 28 January 2003 on public access to environmental information[225], repealing Directive 90/313/EEC). Rules regarding time, conditions, restrictions and charges for requests in this area have been determined, as well as principles regarding which information should be made publicly available ('active publicity'), access to justice and determination of the quality of the environmental information.

Regarding Public procurement matters, the European legislative package consists of: Directive 2004/17 of the European Parliament and of the Council of 31 March

[222] Prof. P. Seipel, "Public Access to public sector-held information and dissemination policy – the Swedish experience", *Conference of Stockholm on access to Public Information, 27*-28 June 1996, http://europa.eu.int/ISPO/legal/stockholm/en/seipel.html; Beers, T. A. L., "National secrecy interests versus public access", *Conference of Stockholm on access to Public Information,* 27-28 June 1996, p.1, http://europa.eu.int/ISPO/legal/stockholm/en/beers.html,

[223] Apart from specific information on each Member State legislation, several surveys on national legislation on access to official documents have been consulted: Kranenborg, H. and Voermans, W., *Access to Information in the European Union. A comparative Analysis of EC and Member State Legislation*, Europa Law publishing, Groningen, 2005; Banisar, D., The FREEDOMINFO.ORG Global Survey – *Freedom of Information and Access to Government Record Laws Around the World*, May 2004, to be found at http://www.freedominfo.org ; Council of Europe, *Replies to the Questionnaire on National Practices in Terms of Access to Official Documents*, Strasbourg, November 2002, Document Sem-AC(2002)002 Bill to be found at http://www.coe.int/T/E/Human_rights/cddh; European Commission, *Overview of Member States' National Legislation Concerning Access to Documents*, Document SG.B.2/VJ/CD D(2000) of 9 October 2000, to be found at http://www.europa.eu.int/comm/secretariat_general/sgc/acc_doc/docs/apercu_en.pdf; European Commission, *Comparative Analysis of Member States' and Candidates Countries' Legislation Concerning Access to Documents*, to be found at http://www.europa.eu.int/comm/secretariat_general/sgc/acc_doc/docs/compa_en.pdf.

[224] UN/ECE Convention of 25 June 1998 on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters

[225] Directive 2003/4/EC of 28 January 2003 on public access to environmental information, *Official Journal* L 041 , 14/02/2003 P. 26 - 32

2004[226], which coordinated the procurement procedures of entities operating in the water, energy, transport and postal services sectors; and Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of contracts for public works, public supply and public service [227]. This issue is further developed in the section of the study especially dedicated to this subject.

The question of the re-use of public sector information has been addressed in the Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information228.

Article 255 of the EC Treaty guarantees the right of access to documents held by the European authorities (European Parliament, Council and Commission) as a fundamental right granted to every European citizen and to every person resident in an EU Member State. The same right is stated in the Charter of Fundamental Rights of European Union (article 42)229. The European Union has also adopted Regulation 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents230. This text details the right of access to documents, lists the exceptions admitted to this right and states very interesting duties of active publicity.

4. What is the relationship of Administration Transparency to the seven barrier categories and associated research questions

Three barriers are relevant when addressing the point of public administration transparency. The four others do not present any link with that subject.

4.1. Digital divides (*Level of importance: significant*)

Results from the stakeholder consultation held by the Commission from October to December 2005[231] indicate that, with regard to citizen involvement, participation and democracy, "there is in general the opinion (64%), that eParticipation and eVoting can help or most likely help closing the democratic deficit. As main barriers are mentioned: lack of trust and security, insufficient access to information and communication technologies and lack of leadership."*[232]*

One of the main issues concerning transparency of public sector information is the digital divides represented by the way knowledge and skills are distributed among

[226] Directive 2004/17 of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors, *Official Journal* L 134 , 30/04/2004 p. 1 – 113
[227] Directive 2004/18/EC of the European Parliament and of the Council 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* L 134 , 30/04/2004 p. 114 - 24
[228] 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 L 345, 31/12/2003 p. 0090 - 0096*
[229] Charter of fundamental rights of the European Union, *Official Journal C 364, 18/12/2000 p. 0001 - 0022*
[230] Regulation (EC) No 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 L 145 , 31/05/2001 p. 0043 - 0048*
[231] eGov Stakeholder consultation (2005) available at http://europa.eu.int/information_society/activities/egovernment_research/index_en.htm
[232] Your Voice on eGovernment 2010, online public consultation; report Jan 2006 V 1.0

users to enable general access to electronic networks and for finding the location of information specifically being sought among the mass of available online information, for example through the provision of easy-to-understand 'meta-data' guides to help navigation through the information that is available, in an appropriate range of languages.

4.1.1 Restrictions on persons authorized to access public sector documents

At present, Spain is the only Member State that restricts the benefit of the right of access to its citizens only. All other Member States grant this right to every natural or legal person, whatever his/her nationality.

Certain Member States demand the demonstration of a specific interest to grant someone a right of access to official documents, whereas free access without proving any personal interest is generally the rule in most countries and in EC Regulation 1049/2001. Italy, for example, restricts[233] the right to ask for documents to applicants who have a personal concrete interest to safeguard in legally relevant situations. The Slovenian FOI Act warrants a right of access to documents only to persons showing a well founded legal interest.

Restrictions for applicants is sometimes foreseen only for certain categories of solicited information. In Latvia and Belgium for instance, restricted information (Latvia) or information revealing an evaluation or value judgement on a natural person (Belgium) may be accessed only by persons who declare the purpose for which they wish to access the information.

4.1.2 Practical difficulties of access

4.1.2.1 Access to, and publication of, documents in electronic media

Not all Member States foresee fully open access to documents in electronic format. Several countries are modifying their legislation to require access to documents in this new format, while others still have paper-based access regimes. When modifying their access regimes, most Member States review at the same time the obligations of Public Authorities regarding the active mandatory publication of public sector information in electronic format.

This evolution transforms the public sector information landscape, making the public sector increasingly aware of the value of its information and the opportunities opened by using its electronic information resources as a new source for improving cost effectiveness.[234] The distinction between raw data and value-added data makes less sense in an electronic context, and in some cases the public sector wants to sell its information directly at profit making prices.[235] The roles of public and private actors may hence be conflicting.

4.1.2.2 Meta-data guides to help locate information

[233] Chapter V (on access to administrative documents) of Act n° 241 of 7 August 1990 establishing new norms in the administrative procedure and right of access to administrative documents.
[234] Burkert, H. "Public Sector Information: some implications for a European information infrastructure", http://herbert burkert.net/ARCHIV/1995-09-00-Vienna.pdf
[235] G. Papapavlou, *op.cit,* p.2 .

A key reason for failing to access information that is available is the lack of information about the accessible information to enable citizens to locate and reach the documents they require.

Regarding information that is passively available, the question is to find the authority one should address to obtain the information. Regarding information that has to be published (active publicity), a citizen needs to know where it has been published in order to find it. Much time can be wasted during the search process because of the lack of international (and, often, even national) public information storage and organizational rules, including clear information about the documents that come within the 'active' category and the ones for which a request is needed.

As already mentioned, the legal obligation to publish such meta-data exists in some Member States' legislation and in the EC Regulation 1049/2001. Several countries ask their public bodies to make publicly available catalogues or registers of the information they hold.[236] Some legislation specifies that these public registers must be accessible on the Internet.[237] All references to documents are to be recorded in the registers identifying the subject matter or a description of the content of the document and its date and its source. Such public registers are certainly a valuable aid to locating and accessing documents, offering an answer to the problem of insufficient accessibility to official information.

4.1.2.3 Cultural barriers

Language can be an important barrier, even when transparency is legally guaranteed in a Member State, as such legislation does not necessarily imply the delivery of information in the language of the person requesting the information, or in English or any other 'international language'.

4.1.2.4 Fees

In certain countries, fees perceived as being too high are charged for access, discouraging requests for information. The Irish law, for example, was amended in June 2003 to impose higher fees "in order to combat abuse of the access rules"[238], which led to charges of 15 EUR for a request, 75 EUR for internal review and 150 EUR for review to the Information Commissioner. Most countries explicitly exclude charging for the costs of searching and retrieving the requested documents, although Ireland and UK impose such costs. For copying documents, France asks 018 EUR per sheet while Austria asks 3,60 EUR per sheet.

4.1.3 Lack of awareness

In all EU Member States, there is a general lack of awareness of the existence of FOI Acts. Even in Sweden, which has had a right of access to official documents for more than two centuries, people are insufficiently aware of their rights and insufficiently exercise them. The Swedish government is aware that[239] " inadequacies exist in terms of knowledge about the public access to information

[236] See above.
[237] See above.
[238] H. Kranenborg and W. Voermans, *op.cit,* p.81.
[239] Cited by Banisar, D. *op. cit.*, p. 82.

principle. Many citizens have insufficient knowledge of these rights, making it difficult for those citizens to exercise them". It therefore launched the 'Open Sweden campaign' in 2002 to increase public-sector transparency, to raise the level of public knowledge and awareness of information disclosure policies and to encourage active citizen involvement and debate.

4.2 Poor coordination (Level of importance: somewhat significant)

The lack of a harmonized regime at EU level with regard to access to public sector information, except for environmental information, has already been highlighted, indicating that the European legal landscape concerning public administration transparency is not uniform. However, some harmonization exists, since the principles laid down in Recommendation R(81) 19 of the Council of Europe of 25 November 1981 have been used as a model by many Member States.[240]

Structural barriers add to the difficulty. For instance, the federal structure of some States accentuates the disparity of access policies. In Belgium, the legal framework is distributed over a federal and several regional levels. In Austria, legal provisions on access to official documents also exist at different internal levels: federal or provincial. In Germany, sectoral laws offer access to specific types of information and some Länder have constitutional provisions and general access laws, with each level adopting different restrictions.

Two areas where differences between Member States or regional levels are specially to be noted are the active transparency and the restrictions to access. Recently adopted or recently modified FOI legislations present two characteristics: their provisions on active transparency are more detailed and they require that the information be available through electronic public network (the Internet). Such provisions are certainly an incentive to eGovernment in the sense that they oblige public bodies to develop electronic public information services, and they favour eDemocracy developments. However, there are clear differences between national laws on this point, with certain laws containing detailed provisions while others are totally silent on the same subject.

Laws and regulations regarding access to public sector information contain rules prohibiting the access to information in some circumstances. Some of the exemptions are very similar in different Member States, but particular legal, historical, political traditions or other reasons result in exemptions differing substantially between Member States,[241] For instance: access can be denied if the

[240] Recommendation n° R (81) 19 of the Committee of Ministers to Member States on the Access to Information Held by Public Authorities, available on http://www.coe.int/T/e/legal_affairs/Legal_co-operation/Administrative_law_and_justice/Texts_&_Documents/Recommendation(81)19.asp. Recommendation Rec (2002) 2 on Access to Official Documents, adopted by the Committee of Ministers of the Council of Europe on 21 February 2002, though no legally binding instrument, aims too at harmonising national legislation in the field of access to official documents.

[241] For example, the Finnish law protects "personal integrity and other important personal interests in health care, social services, taxation or public supervision" (Act n° 621/99 on the Openness of Government Activities of 21 May 1999) while such precision is not present in other laws. Greek law ,for example, foresees an exception to access when "the document concerns the private or the family life of a third party" (Article 5 of Act n° 2690/1999 Administrative Procedure Code, of 9 March 1999); Danish law states that the right of access to administrative documents shall not apply "to personal data" (Danish Access to Public Administration Files Act n° 572 of 19 December 1985 in 1991 and in 2000); the Italian law protects "the privacy of third parties, persons, groups and

request is *abusif* (excessive) or obviously formulated too vaguely (in Belgium); seems obviously unreasonable (in Austria and Ireland); or is vexatious (in UK). In some countries (e.g. Hungary[242], Sweden or the Czech Republic[243]) secrecy requirements relating to information access are highly detailed in a Secrecy Act, while this is not the case in other countries.

With regard to constraints on access, some harmonization exists since the contracting parties to the European Convention of Human Rights must abide by the requirements of Article 10, paragraph 2 of the Convention when restricting access to public documents. Such restrictions have to be prescribed by law, be necessary in a democratic society and have a legitimate aim described in this Article such as: being in the interests of national security, territorial integrity or public safety; for the prevention of disorder or crime; for the protection of health or morals; for the protection of the reputation or the rights of others; for preventing the disclosure of information received in confidence; or for maintaining the authority and impartiality of the judiciary.

4.3 Lack of trust *(Level of importance: somewhat significant)*

Trust is not only linked to security and authentication questions but also to transparency. Public administration transparency is considered today as a fundamental condition for public trust in government activities, and notably in eGovernment services. This means that access by citizens and private bodies to government information plays a role in building trust. Section 4.1 has examined some key constraints on access to information from the user's point of view. This section examines obstacles to building trust raised by a lack of openness by public administrations.

4.3.1 Need for changes of government culture

In many European Member States, there is a lack of tradition for openness. Even where legislation now exists to underpin greater administrative transparency, a change of internal culture of government bodies is still needed to achieve this. The following are some examples of this:

- A study conducted in 2001 and 2002 in the Czech Republic[244] pointed to problems with "the overuse of commercial secrets and data protection as justifications for withholding, unjustified denials by agencies that claim that they are not subject to the act or simply ignore the law, and a failure of agencies to provide segregable information" [245].

- In Latvia, problems of practical implementation of the FOI Act have also been signalled. In 2001, following a survey of 200 ministries, it was found that "the

---

enterprises" (Chapter V – on access to administrative documents – of Act no 241 of 7 August 1990 establishing new norms in the administrative procedure and right of access to administrative documents).

[242] A list of 149 categories of information to be considered as 'State secret' in annexed to the Act LXV on State Secrets and Official Secrets.

[243] 28 types of information listed as subject of being classified into four levels of classification

[244] Open Society, b.a., Free Access to Information in the Czech Republic, August 2002, available at http://www.otevrete.cz/index.php?id=142&akce=clanek

[245] Banisar, D, op. cit., p. 25.

Latvian government has not devoted sufficient resources to ensuring compliance by state institutions to the laws governing access to information"[246]. A follow-up survey held in 2002 and 2003 identified remaining problems of resources, training and education of public authorities. Local government officials were still largely unaware of their responsibilities, even if central government institutions and courts had gained knowledge of transparency new rules. Only one third of the requests received a response in the legal time frame.[247]

- In Slovakia, the Citizen and Democracy Association checked in 2002 the correct implementation of the Act on Free Access to Information. It found that trivial information was usually provided but more 'problematic information' such as contracts and privatization was most of the time withheld. Moreover, solicited documents were often arbitrarily refused or given only after an attorney's intervention.

- Even in Sweden, as discussed in Section 4.1.3, they have to face insufficient implementation of access to information rules. A distinctive feature is that it was the government itself that identified a problem of insufficient openness in practice when it launched its Open Sweden Campaign in 2002. The Swedish government said it found that "clear signals from the public, journalists and trade unions and professional organization indicate that inadequacies exist in terms of knowledge about the public access to information principle and with respect to its application. Examples of such inadequacies include delays in connection with the release of official document, improper invocations of secrecy […]"[248].

4.3.2 Insufficient information made publicly available because of legal restrictions of access to official documents

As discussed earlier, Blockages to eGovernment created by varying exemptions to the right of access determined by law or other rules in the Member States and in Regulation EC 1049/2001 concerning European authorities can originate from the definition of the scope of national and EC legislation on access to documents or from the list of exceptions admitted to the principle of access.

Such restrictions can be classified as follows:[249]

- Exemptions in the interest of State (national security, public order, economic interests, international relations, legislative procedures, , etc.), for example:
  - Some information is delivered to the State only for statistical purposes. This information is sometimes not anonymized at the time of collecting the information, so cannot be delivered under access legislation.[250]

[246] Delna, "A Survey of Access to Information in Latvia", Transparency International, available at http://www.delna.lv
[247] Banisar, D., *op. cit.*, p. 52.
[248] Cited by Banisar, D. *op. cit.*, p. 82.
[249] Papapavlou, D. "Public sector initiatives in the European Union, Unesco Infoethics 2000", p. 7, http://webworld.unesco.org/infoethics2000/

- Exemptions in the interest of third parties (Intellectual Property Rights, privacy, commercial secrets, judicial procedures, etc.), for example:

  - When protected by IPR, information will be delivered to the person requesting a copy of a document only with the authorization of the author.

  - As the Berne Convention (art. 2 (4)) gives national legislations the discretion to determine the intellectual property protection to be awarded to official texts of a legislative, administrative or judicial nature, a disparity may arise in accessing (copyrighted[251] or public domain[252]) official documents in different Member States.

  - When a document relates to private information about a person, it will often not be delivered to a third party without the authorization of the concerned person[253].

- Exemptions to protect the decision-making process (e.g. preliminary or 'internal use' information).

- Exemptions to avoid unreasonable workload in the administration concerned (e.g. information already published, excessive requests, vague requests).

Most laws require a 'harm test'. This examines whether access may, or shall only be, refused as far as disclosure would harm certain protected interests. Some Member States are stricter than others when applying this test. For instance, in some cases access is to denied when disclosure could harm (e.g. Czech Republic), would harm (e.g. Estonia, Hungary, Lithuania, Sweden), is reasonably expected to harm (e.g. Ireland) or would cause a concrete damage (e.g. Italy) a protected interest.

In addition, some exemptions are mandatory (their occurrence prohibits the access without any discussion), while for others the public authority involved must balance the public interest in openness and the interests related to preserving secrecy. This 'balance test' (also called 'public interest test') is often performed differently in different cultures.

4.3.3. Insufficient and divergent legal duties of active transparency

Access to public sector information can be split up in two categories:

- passive: rules determining the information to which access must be given upon request of a citizen, business or another public authority; and

- active: rules regarding information that public authorities have to make spontaneously publicly available without any need for request.

---

[250] For example, see the Danish Access to Public Administration Files Act n° 572 of 19 December 1985 revised in 1991 and in 2000; the Spanish Law 30/1992 on Rules for Public Administration of 26 November 1992, modified by law 4/99 of 13 January 1999.
[251] This is the case in UK.
[252] This is notably the case in Finland, Belgium and France.
[253] This is notably the case in the Slovak law (Act n° 211/00 of 17 May 2000 on Free Access to Information) and in the Belgian law (loi du 11 avril 1994 relative à la transparence de l'administration).

Most EU Member States having laws on access to official documents include duties of government agencies to publish on their own initiative or make available certain categories of information. Instead of being a constraint on eGovernment, these provisions foster development of eGovernment, especially when they require the accessibility of information on the Internet. Serious divergences among national legislations are worth noting in this regard.

A majority of countries demand their public bodies to release information on their structure, functions, duties, activities, internal rules, procedures or practices, regulations and their interpretation.[254] Certain national laws[255] also provide that each authority has the duty to disclose public interest information in their field of activities.

Recently adopted or recently modified FOI legislations require certain kinds of information to be made actively available through the Internet, for example:

- The Estonian Act contains significant provisions regarding electronic access and disclosure of public sector information. Public bodies "have the duty to maintain websites and post an extensive list of information on the Internet including statistics on crime and economics; enabling statutes and structural units of agencies; function descriptions of officials, their addresses, qualifications and salary rates; information relating to health or safety; budgets and draft budgets; information on the state of the environment; and draft acts, regulations and plans including explanatory memorandum".[256]

- In Poland, public authorities are required to create a Public Information Bulletin to allow access via computer networks to information about their policies, legal organization, principles of operation, content of administrative acts and decisions, and public assets.[257]

- Article 5 of Slovakian law contains an extensive list of information that has to be disclosed in a way that enables mass access. By 'mass access', the law means accessibility by means of telecommunications, especially through the Internet.[258]

- In Slovenia, public authorities have the duty to release information of public character on the Internet. This includes: consolidated texts of regulations relating to the activities of the public body and its programmes, strategies, views, opinions, studies and other similar documents; proposals for regulations, programmes and strategies; all publications and tendering documentation in accordance with regulations governing public procurements, information on administrative services; and other information of public character.[259]

[254] Such requirements, or parts of them, are present in Belgian, Czech, Estonian, Finnish, French, Irish, Lithuanian, Polish, Portuguese, Slovakian, Slovenian, UK laws.
[255] Hungarian law, for example. Also, the Dutch Act on public access to government information of 31 October 1991 states: "If disclosure of information on the policy of an administrative authority is in the interest of effective, democratic governance, the authority must on its own initiative disclose the information."
[256] Public Information Act of 15 November 2000, RT I 2000, 92, 597.
[257] Act on Access to Public Information of 6 September 2001.
[258] Art. 4, § 2 and 6, § 1 of Act n° 211/00 on Free Access to Information of 17 May 2000.
[259] Art. 10 Act on the Access to Information of Public Character of 25 February 2003.

- Article 5, § 2 of the Greek Constitution stipulates: “All persons are entitled to participate in the Information Society. Facilitation of access to electronically handled information, as well as the production, exchange and diffusion thereof constitutes an obligation of the State, always in observance of the guarantees of Articles 9 [protection of a person’s home, private and family life], 9A [protection of personal data] and 19 [secret of correspondence].”

- EC Regulation 1049/2001 provides that the European institutions are compelled as far as possible to make their documents directly accessible to the public in electronic form or through a register. In particular, legislative documents, which means documents drawn up or received in the course of procedures for the adoption of Acts which are legally binding, are to be made accessible. Where possible, other documents, notably documents relating to the development of policy or strategy, should also be made directly accessible.[260]

- Several countries ask their public bodies to make publicly available catalogs or registers of the information they hold.[261] Some legislation specifies that these public registers must be accessible on the Internet.[262]

- International, European and Member States legal texts relating to access to environmental information provide for a wide electronic disclosure of that kind of information.

[260] Art. 12 EC Regulation 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.
[261] Estonia, France, Latva, Lithuania, Slovenia, Spain, Sweden.
[262] Slovenia, Belgium (Flamish Regional level), EC Regulation 1049/2001

Relationships between Public Administrations, Citizens and other ICT Actors
Dr Julián Valero Torrijos, University of Murcia, Spain

1. Description of the area

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, on the one hand it is necessary to ensure that they are able to gain access to electronic public services since the use of ICT may involve new and unexpected obstacles for their relationships with public authorities. On the other hand, hat governments may adopt a too timid policy to promote eServices, in which case, the use of ICT will not be perceived as an advantage by users since many of the possibilities offered by private companies in their regular activities – such as bank transfers, sales of travel tickets and general access to information – are not available in the eGovernment services.

Some other questions must be also taken into account in this area, especially those connected to the relationships between public administrations and ICT companies. Since many of the actions in the field of eGovernment demand a high investment in technology-related resources - both in terms of hardware/software and specialist personnel – the collaboration of those actors is essential as most public administrations haven't got the appropriate means to meet these requirements. Nevertheless, it is important to ensure final decisions are taken by the public authorities when necessary in order to prioritize protection of public interests. This demand becomes especially relevant when defining technological standards for ePublic Services.

2. Why could there be barriers to eGovernment in this area?

Without a general right to use online services in all their relationships with a public administration, citizens may lose confidence in eGovernment, thereby hindering the demand for, and establishment of, new eGovernment services. For instance, the ICT-enabled services frequently made available to citizens may allow only for a narrow range of applications that have been previously and expressly sanctioned by the administration concerned (e.g. to contact the public administration, to return an application form, get information or receive notification of an administrative decisions). As a result, such citizens may find that the only ICT-accessible public services available to them are not those they considered to be most valuable to their own lives. In some circumstances, it may be impractical (e.g. too costly) to implement multi-channel access to a public service, in which case it may be necessary to impose the use of ICT as the only means of contacting a public administrations. But this decision can only be adopted when it does not imply discriminatory consequences and ensures access to the public service is available to everyone who needs it.

As for the relationships with ICT companies, there are several potential risks that may involve some barriers from the legal point of view. For instance, it is critical that decisions about the design and use of ICTs are not biased toward a particular firm or technology (e.g. a certain operating system or web browser) since they might be

contrary to the rules on free competition guaranteed at a European level and by national regulations on public contracts. Technological neutrality must also be extended to those services provided by Trusted Third Parties when their participation is needed to put in action eGovernment solutions. Otherwise, citizens will be obliged to use only certain commercial products and/or services when there is no technical reason to justify this limitation.

3. What is the European context for this area, including legislation, policy statements, institutional arrangements relevant to this topic?

The European context in this area is analyzed in relation to the perspectives of different key actors.

3.1 The perspective of citizens

Although the use of ICT means does not necessarily result in a better a better and more efficient public administration, technological modernization offers a unique opportunity to achieve this essential challenge for modern and democratic public bodies, as the Report *eGovernment in the EU in the next decade* highlights. This linking must be emphasized as many Member States are adopting legal obligations for their authorities and civil servants to achieve good public administration standards and, which recognizes a related right for citizens in received such services. Moreover, in some cases this right is guaranteed at the Constitutional level, as in the Finnish Constitution or the Treaty Establishing a Constitution for Europe – commonly referred to as 'EU Constitution' – which is subject to further ratification processes. Many of the principles imposed by this right may be reached more easily through eGovernment tools, such as the right to have one's affairs handled within a reasonable time, the right for citizens to have access to their files or the right to general access to documents.

Another of the pressing demands reinforced by these new principles and many other relevant initiatives on eGovernment is the need to go more deeply into a citizen-focused government approach. As the 2003 *Capgemini eEurope eGovernment Report* warns: services must be developed where citizens receive value in return for their taxes, rather than the services that mostly interest governments. The 2005 *Capgemini Report* also stresses this perspective, although it concludes that greater improvements have been made in electronic services addressed to companies than to citizens. However, this user-centred philosophy must be supported by legal and institutional changes, as the European Commission's (2005a) *CoBrA Recommendations to the eEurope Advisory Group* has outlined.

The issue of accessibility to eGovernment services must also be considered as a priority. Legal questions about this should be taken into account with some urgency, although online public services have a long way to go before they are fully accessible and inclusive (and this objective could be considered as Utopian for economic reasons, as explained the European Commission (2004b) document on *Multi-channel delivery of eGovernment services*). Even if complete usability for all groups cannot be reached, in many countries restrictions on access to online services through poor design is illegal and in others considered discriminatory (see EPAN 2005: *eAccessibility of public sector services in the European Union Report*).

Therefore, as a rule, multi-channel provision must be considered as the fairest option in order to guarantee the universal access to public services, including at least and one electronic and one traditional avenue.

3.2. The perspective of public administrations and ICT companies

According to the IPTS (2004) document *eGovernment in the EU in the Next Decade: The Vision and Key Challenges*, eGovernment will need to be not only more user-centric but also more networked. The involvement in designing and implementing eGovernment services by an increasing number of public, private and social actors and intermediaries at EU, national, regional and local levels – as a consequence of a clear tendency towards political decentralization – demands a serious effort in order to strength coordination and collaboration. One of the most urgent reasons for this premise is related to interoperability, both from a technical and an organizational perspective since. As European Commission (2003a) *Communication from the Commission to the Council and the European Parliament on Interoperability for Pan-European eGovernment Services* has outlined, national programmes in this field have encountered serious legal hurdles when trying to simplify processes to support more efficient interaction. Moreover, as explained in the IDABC (2004b) *European Interoperability Framework for pan-European eGovernment Services*, the diversity of national legal and administrative systems may become an additional and very relevant blockage to achieving this target, especially at the European level. Promoting the use of open standards, as recommended at the *eGovernment Policy Stakeholder Meeting* held in Brussels on 21 September 2005, and establishing technical standardized criteria at the European level – perhaps through the projected *European Institute of Technology* – may be considered as inevitable measures.

eGovernment services implementation demands close cooperation between public administrations and ICT companies because of the technological difficulties of this process. However, this collaboration must respect some important legal exigencies, specially those related to requirements for free service provision imposed by the EU Treaties with a general scope and those fixed by European and national regulations on public procurement. An example could of the context-specific implications of these requirements is that those Member States deciding to offer digital signature services associated with electronic Identification (ID) Cards must guarantee the use of alternative digital certificates provided by other public or private Certificated Service Providers; otherwise, Article 4.2 of the *Directive 1999/93/CE on a Community framework for electronic signatures* would be infringed.

4. What is the relationship of this legal area to the seven barrier categories and associated research questions?

The following summarizes the degree to which each of the seven barrier categories used for this research are to legal aspects of relationships between public administrations, citizens and other ICT actors.

Leadership failures: *Somewhat significant*, since leadership is an important element in helping to focus eGovernment projects on the needs of citizens and companies and to solve interoperability problems, specially when the leading role is played by

national authorities. Nevertheless, such leadership is not essential to achieving these goals.

Financial inhibitors: *Somewhat significant*, particularly regarding the high cost of implementing multiple channel systems and making eServices available to different disadvantaged groups in order to achieve the inclusivity goal by recognizing the right for citizens and companies to have a choice in how they make contact with public bodies (e.g. online, face-to-face, post, email, telephone).

Digital Divides: *Significant*, mainly for two reasons. Firstly, when eGovernment services are designed mainly to solve internal administrative problems rather than being conceived to serve the needs of citizens, business and other stakeholders, they are likely have poor usability interfaces and interactions. Secondly, compulsory use of electronic public services may raise constitutional or legal problems if they impede the right of certain groups or individuals to have access to those services.

Poor coordination: *Very Significant*, since coordination is one of the most essential factors in implementing networked electronic public services and in the more general exchange of information between public administrations and other stakeholders. Poor coordination becomes particularly relevant as a barrier when a public organization is based on a decentralized model that supports networked governance processes as effective coordination is then a critical requirement in the provision of high quality public services.

Workplace and organizational inflexibility: *Significant*, since these blockages and constraints focus on the internal perspective of eGovernment services and not in the needs of citizens, companies and others who are their final users.

Lack of trust: *Significant.* The absence of a wide recognition of citizens' right to contact public administrations through electronic means may involve a lack of trust in eGovernment services, specially if compared with those eServices offered by private companies. Likewise, it is certainly relevant to assure the implementation of eGovernment services with a strict respect of the legal requirements for the use of ICT means since, otherwise, a serious risk to their validity and effectiveness can be arisen and, therefore, citizens will not trust this channel since their rights might be seriously affected.

Poor technical design: *Very Significant*, since these kind of incompatibilities are usually directly connected to inadequate relationships between public administrations, citizens and other actors, like ICT companies.

5. What are the main legal problems in this area?

5.1. The absence of legal obligations to provide electronic public services

As discussed in Section 2, the lack of confidence in eGovernment caused by the availability of only a narrow range of predetermined services could be addressed by a general right – legally assured – to use online services in all relations with a public administration. This should promote a wide understanding of eGovernment services available to citizens and, as an essential demand, the legally guaranteed opportunity

to contact the public administration by electronic means to pose any request for information and obtain an effective and quick answer.

Unless there is a clear legal obligation to offer certain electronic public services, public administrations are likely to use their wide discretionary power to prioritize which relationships with citizens can be undertaken electronically. As public financial resources are limited, and there is strong pressure to use that money in the most efficient and effective way, the intensity of technological eGovernment modernization may vary according to factors other than legal dimensions, such as political considerations, particularly in the case of local administrations. This can lead to eGovernment being seen as a lower priority than other investments, such as building a new and modern hospital before promoting eGovernment services. Moreover, technological modernization of public administrations is a very complex process and may demand relevant changes in the organizational culture and habits of civil servants and authorities, which makes it easier to emphasize political options with a lower level of risk and difficulty.

However, public administrations must adapt their activity to take account of technological innovations relevant to exercising their functions since. Otherwise, there will be a high risk of inefficiency in the operations for which they are responsible. This potential problem must also be assessed from a democratic perspective, specifically, taking into account the degree of satisfaction of the groups targeted by public services. Given that many citizens as well as businesses are increasingly getting used to ICT tools in all other activities of their life in an information society, at least national, regional and medium/large local Administrations should adopt ICT-enabled solutions not only for their internal administrative activity but also to give a better service to their customers. If they don’t assume this obligation spontaneously, as a last resort after investigating other options consideration should be given to introducing legal obligations to achieve eGovernment aims, such as those egovernment objectives set for the EU (see Part 1). This could offer a degree of juridical security as this kind of measure can enable citizens and companies to know exactly what they should expect from eGovernment services and therefore will be able to demand such provision to their satisfaction.

Despite the relevance of this barrier for eGovernment progression, it cannot be considered as a severe one since the reluctance of public administrations to offer new and more useful electronic services may be solved through legal changes that fix clear obligations in a way that overcomes their lack of interest using measures that can usually be adopted by the administrative organization concerned. Public reports ranking the level of electronic public services supply are a useful technique for reaching this goal, although its methodological limitations must be taken into account, specially when they have a European scope. For examples, the conclusions of such reports cannot be exhaustive since they cannot bear in mind adequately the real situation of eGovernment services at regional and, above all, local levels.

Therefore, the establishment of legal obligations in order to provide useful electronic public services must 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 this decision. A

relevant example is the European initiative to promote the compulsory use of electronic means in the field of public procurement through Directives 2004/17/EC and 2004/18. The positive results of this obligation has rapidly appeared, for instance with some Member States, such as France, having already adapted their own legal framework and gone even further than what has been recommended by the European Directives, as explained in the country examples of eProcurement section of our project's website.

5.2. Interoperability problems

As previously explained, one of the main challenges for public bodies in this field is to achieve a more networked eGovernment service since, in many cases, administrative decisions can be adopted only using information that is in the responsibility of other administrative units. If a higher level of efficacy is expected when using ICTs, then it will be necessary to automate this kind of communication; otherwise, it won't be possible to make the most of many of the advantages offered by technology, such as the speed to process high amounts of information, accuracy in searching process of data and updating of files. This requirement has been highlighted by the *eEurope Action Plan* as it was recognized as a precondition for European eGovernment services and as a key issue in providing better services for citizens and companies and to ensure more effective implementation of EU policies. To achieve this, interoperability – especially at a national level – is an elementary requirement in building build European electronic services (e.g. see European Commission 2005b: *Study on Interoperability at Local and Regional Level*).

As the European Commission's (2003a) *Communication from the Commission to the Council and the European Parliament on Interoperability for Pan-European eGovernment Services* noted, some Member States have encountered legal hurdles when trying to satisfy this requirement, which becomes a serious obstacle not only for developing national eGovernment programs but pan-European ones as well. This technological problem faces an additional difficulty from the political point of view: many Member States are territorially decentralized and, therefore, fragmentation may become a relevant obstacle for this purpose when local and regional Administrations develop their own eGovernment systems. Moreover, as a last resort, this inconvenience may even have relevant consequences at the supranational level since European eGovernment services are usually based on the information provided by national, regional and local authorities.

Another inconvenience must also be overcome with relevant consequences from a legal point of view. Public administrations usually commission private companies to design the information systems and software required to supply eGovernment services, and this inevitable and profitable collaboration may reveal a new problem in seeking to guarantee interoperability if public interests are not properly guaranteed. For the correct development of eGovernment solutions it is therefore essential to adopt some legal measures that allow a high level of technical interoperability based on elementary exigencies of standardization, both for public and private actors. Even more, from this perspective, it must be emphasized that public-private partnerships (PPIs) are increasingly required in many economic and social fields, with substantive general implications (see IPTS 2004). An elementary demand of collaboration with private sector in our digital society requires efficient solutions for the potential

inconveniences derived from this circumstance although, they may not be too forceful from the legal perspective.

At the European level, compulsory legal solutions for these questions are certainly inadequate and, therefore, other measures must be considered, such as those already put into action through the European Commission's (2003a) *European Interoperability Framework for pan-European eGovernment Services*, where it is clearly remarked that impositions on Member States are not fitting and technical recommendations can be seen only as a proposal. Therefore, at this level, the analyzed barrier has serious inconveniences to be overcome in a satisfactory way from a legal and compulsory point of view, as the EU has no direct competences to help achieve this goal.

On the contrary, more severe actions can be taken by Member States as national authorities have concrete legal tools at their disposal, especially if all of them are put in action together. First, national authorities should promote soft law measures like the adoption of clear technical standards by the specialized committees in charge of this subject. The German initiative can be considered as a good example: the Federal Ministry of the Interior has recently published version 2.1 of its Standards and Architectures for eGovernment Applications (SAGA), the German e-government interoperability framework, which are periodically revised and actualized by the Advisory Agency for IT in the Federal Administration (KBSt), an inter-ministerial agency aimed at ensuring that the federal administration optimizes its use of information technology.[263]

Even when these conditions cannot be imposed on regional and local public administrations, it is possible to make financial support to their eGovernment programmes – and other ways of collaboration – conditional on the observance of these requirements, although a wide agreement between all public bodies concerned is certainly preferable. This has been the case in the Belgian eGovernment's strategy, which seeks to create a single virtual public administration while respecting the specificities and competences of all government bodies and administrative layers. An agreement was signed in March 2001 by the federal, regional and community authorities to lay down the framework of this cooperation and, particularly, the commitment by all layers of government to use the same standards and the identification infrastructure.[264] This cooperative approach has also inspired the initiative AOC[265] in the Spanish Region of Catalonia, a good example of collaboration between all administrative levels, particularly regional and local, which has been internationally recognized as a nominee for the e-Europe Awards in 2003. One of the main objectives of this project is to share software for eGovernment services with local administrations and, indirectly, contribute to a higher interoperability.

Some other legal measures should be adopted, although their efficacy in removing blockages to eGovernment progress is relative and diverse. On the one hand, national regulations on public procurement should established a legal obligation to give preference, among other circumstances, to the use of interoperability standards

[263] Further information on this example can be found at http://europa.eu.int/idabc/en/document/4713/336
[264] Further information on this example can be found at http://europa.eu.int/idabc/en/document/1359/386
[265] http://www.cat365.net

when selecting the companies that are going to design the software and information systems. Moreover, a general obligation of compatibility for all public administrations should be legally adopted in order to force them, when possible, to use standardized software solutions, although this may not be as effective as desired in practice.

5.3. The absence of a general right to use ICT from the perspective of citizens and companies

As numerous European documents and reports have shown, although the supply of electronic public services has considerably increased in recent years, it can be stated that there is still a need for going more deeply in this direction in order to put "*Administration electronique au service du citoyens*" (Chatillon and Marais, 2003). This new model implies a concept of eGovernment provision based on the effective meeting of the needs of citizens as a priority above satisfying the public bodies' requirements. It is significant that not only do the best-established electronic public services typically refer to their fulfillment of internal administrative interests, such as income tax, rather than external needs (Capgemini, 2003) but that a significant administrative preference is shown for those services addressed to companies rather to citizens (Capgemini, 2005). It is clear that this imbalance can be explained from this perspective since, usually, relationships between public administrations and companies are characterized by a higher frequency and complexity, as well as a better profitability from a fundraising perspective. Once again, the proposed helpful paradigm must be demanded and legally assured not only to satisfy individual requirements but, especially, to improve the democratic legitimation of public bodies through their activity.

The absence of a general right for citizens and companies to use electronic means to contact public administrations can be considered as a serious risk for undermining their confidence in eGovernment and, in many cases, can lead to a lack of interest in this channel if their interests are not met. Although some of the implications of this problem have already been examined from the perspective of public administrations, we must highlight specific nuances of this question from user's point of view that are directly related to the significance of the barrier. We are indeed faced with a greater difficulty, since it is up to public administrations to decide about the supply of electronic services and, therefore, they tend to give priority to their own technological modernization needs to enable citizens to contact them and obtain information online. Users can oblige public administration to offer this possibility only when it is legally recognized as their right.

Overcoming this barrier is not easy at a European level since the most useful services for companies and, above all, for citizens are under the responsibility of national, regional and local authorities. However, basic freedoms guaranteed by the European Union Treaty – and particularly the achievement of a European common market – may be considered as a relevant argument in order to adopt some measures that necessarily involve the use of electronic public services, specially for those companies that are established in a Member State and desire to carry out their activity in other different one. Anyway, in the main role of citizens in solving these inconveniences relates to national public bodies and, specifically, to the authorities – in many cases national or regional Parliaments – with the competence to establish a general right for them to the use of eGovernment tools.

It is obvious that the scope of this measure must be adequate to the concrete circumstances of the entities concerned and the complexity of the activities concerned, but in the information society some elementary obligations should be adopted in order to promote eGovernment solutions. Regardless of the specific needs of smaller local administrations, where financial limitations could be argued, all other public administrations should be legally obliged to offer at least two essential eGovernment services: online access to public information and the ability to obtain application forms through electronic means. These may be considered as the most useful services for users, both citizens and companies, and the organizational, technical and financial effort required for provide them is not disproportionate, especially if we bear in mind that the relevant public administrations already have a website and use ICT in their everyday activities.

Two national examples offer a reference in this field. The Finnish Act on Electronic *Electronic Service and Communication in the Public Sector*[266] obliges those authorities in possession of the requisite technical, financial and other resources to offer the option of sending a message to a designated electronic address, or another designated device, in order to lodge a matter or to have it considered. On the other hand, the Italian *Codice dell'ammnistrazione digitale*[267] has established: the minimum set of contents and services available on national public administrations websites; the right to communicate by e-mail, namely for the exchange of documents and information; the need to accept online payments from citizens and businesses; a citizen's right to demand that public administration bodies use electronic means in their day-to-day relationship with their publics.

5.4. Compulsory use of ICT and access to public services

The promotion of electronic public services cannot be focused on compulsory use of ICT by the citizens because that kind of measure may infringe the principle of equity in the access of users to public services. As the IPTS (2004) report on eGovernment in the EU in the next decade warns, 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 only be considered fair – and sometimes constitutional – if there are no unjustified limitations on the exercise of citizens and companies' rights or the fulfilment of their obligations. Precisely because of the existence of a digital divide that affects a wide range of groups in several Member States, it is 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. As the European Commission (2004b) study *Multi-channel delivery of eGovernment services* emphasizes, "if a user is legally entitled to a service, the administration is legally required to deliver the service".

It must be emphasized that general solutions at a European level cannot be adopted since the practical conditions for accessibility ICT-enabled services are different in each Member State and for each group of users. These determining factors must be taken into account when establishing new legal provisions about this issue in order to

[266] Chapter 2, sections 5 and 7. This Act is available at
[267] Further information on this example can be found at http://europa.eu.int/idabc/en/document/4820/5707

avoid discriminatory consequences, which may even involve the impossibility of accessing public services for some citizens or, even more, force them to fail in the fulfilment of their legal obligations. The *Spanish Administrative Procedure Act* can be considered an adequate way of combining these requirements in a proportionate way since the compulsory use of ICT is established only for big companies and public administrations, although a Ministerial Order[268] can oblige to other groups of users as well if that measure does not involve restrictions or discrimination.

5.5. The absence of legal obligations in order to make eGovernment services available

One of the main problems for users when trying to use eGovernment services is not to be have access to them because of an inappropriate design of the software or because the services can be used only under unfair conditions. Diverse situations must be analyzed regarding this barrier since the legal solutions that can be adopted vary greatly. For example, we can face a problem of access by disabled citizens, scenarios where access is too difficult for technical reasons or cases where technological neutrality has not been respected and, therefore, it is impossible to use an electronic service unless certain software or equipment is used. Overcoming these problems would be assured if legally clear obligations for public administrations were established but, as a last resort, it is up to each public body to solve these inconveniences in an appropriate way. Therefore, if there is an adequate legal framework to face these issues or the appropriate administrative decisions have been adopted, these barriers must only be considered as being perceived ones.

Regarding disabled citizens' access to electronic public services, it is important to warn that the recent European Commission's (2005d) *Communication on "Electronic Accessibility"* warns about a lack of consistency in this field and, therefore, considers that there should be an improvement in the consistency of accessibility requirements in public procurement contracts in the ICT domain, although Directives 2004/17/EC and 2004/18/EC contain already clauses referring to the inclusion of persons with disabilities and older people. This document also recognized that there should be a better use of the 'e-accessibility potential' of existing legislation. Since it is impossible to enable access by everyone to every eGovernment service, except over the course of years, these services are usually offered as an option for disabled citizens and, therefore, alternative distance channels should be offered in some cases to assure access to public services in a more appropriate way.

From a legal point of view, it is clear that 'soft' provisions included in the aforementioned Directives may be completed, as some Member States have done, in order to tighten the accessibility conditions for disabled people, as shown in the document *eAccessibility of public sector services in the European Union*, where precise information about the legal situation in nine countries is summarized. The German option must be highlighted since *The Act on Equal Opportunities for Persons with Disabilities*[269] has introduced the right to legal action taken by any association recognized under this Act. Not going so far, *Austrian Act on*

[268] 18th Additional Provision. This Act is available at http://www.map.es
[269] Available at http://www.cabinetoffice.gov.uk/e-government/resources/eaccessibility/index.asp

eGovernment[270] and *Spanish Act on Information Society Services*[271] establish a general obligation for public administrations in order to make available for disabled citizens the information contained in their websites and authorizes them to impose these conditions on the companies that design them. This last indication is certainly relevant since public administrations should adopt it in every case when approving technical specifications in the field of public procurement, particularly with reference to international standards such as the W3C WAI Guidelines; otherwise, no obligations will be assumed by the companies in charge of designing websites or software for providing eGovernment services.

The design of eGovernment systems can also become an obstacle for the relationships between public administration and private individuals as it hinders the utilization of software or operating systems owned by the latter, especially if they are obliged to purchase a licence for certain commercial products and cannot use other common programs, including free open source software. So, it is essential to ensure legally the technological neutrality of the applications used to transmit administrative information and establish online relationships between public administrations and citizens. This should be expressly guaranteed by the rules regulating the contracts between public administrations and the enterprises that create the software.

6. Analysis and assessment of the main research questions from a legal perspective

The referred problems oblige us to face some relevant and concrete questions in order to propose effective legal measures to remove hindrances to the development and consolidation of eGovernment services. Although a more in-depth analysis will be done during the following months, it is possible to offer an initial assessment of their relevance and the actions that should/could be adopted to overcome their inconveniences.

6.1. Is there a new generation of 'digital rights' emerging?

eGovernment offers a new dimension of citizenship with regard to the relationships with public authorities and the way citizens exercise their rights. The legal recognition of this new generation rights – such as access to public communication networks, public information, e-public services, e-digital identity, the right not to present documents that are already in the hands of public authorities and the right to 'good' administration – is not always as clear, which may make it difficult for citizens' to make demands to improve their the effectiveness of eGovernment services.

The acceptance of these rights does not always depend on national authorities since regional and local levels can frequently oppose their autonomy in order to give priority to other issues, sometimes for financial and organizational reasons. General obligations for all public authorities should be promoted in this field by Member States using their competences , although they must bear in mind the degree of technological advance in each society.

[270] http://europa.eu.int/idabc/servlets/Doc?id=21448
[271] http://www.lssi.es

6.2. Are governments able to mandate use of electronic services, and in which circumstances?

As a rule, promoting eGovernment services cannot be done by a restriction of the ways citizens can contact with public authorities, particularly when this relationship may become impossible. Although some nuanced arrangements could be made in the case of certain Member States, there is a general obligation of no discrimination in most of member States that prevent Governments from ruling out a direct and personal contact with citizens since many social groups have no access to electronic means. Even more, if this decision does not take into account this constraint, citizens may not be able to exercise their rights and fulfil their obligations.

Therefore, EU harmonization is not possible since concrete social, economical, cultural and technological circumstances of each nation lead to different requirements and decisions in different contexts, which therefore remain at the national or regional level. Alternative systems may be suggested by the EU, for example the use of intermediaries such as civil servants or private and specialized agents, when public authorities opt to promote the use of ICT not only from an internal perspective but for the relationships with citizens.

6.3. How do EU regulations block or encourage intermediaries or other third-party providers of eGovernment services?

Usually, EU regulations have as their main objective to facilitate providing services across all Member States and, therefore, they try to promote fair competence and private enterprise. Even more, they do not usually establish over restrictive regulations for different contexts since, on the one hand, they have no direct competence at more local levels and, on the other hand, there is a great diversity among Member States in this field. As an example, the eCommerce Directive has not been conceived to be applicable to the e-activity carried out by public bodies.

Therefore, the main legal problems for technological intermediaries come from national regulations that are not adapted enough to the singularities of ICT and public authorities. Nevertheless, some Directives have not achieved the establishment of appropriate measures that could facilitate more flexibility in ePublic Services provision (e.g. digital signatures) and this may become an obstacle for intermediaries.

6.4. What factors are inhibiting the establishment of innovative financing mechanisms?

From the perspective of public–private partnerships, the inflexibility of public procurement regulations is certainly one of the most relevant inconveniences, particularly because of the singularities and restrictions of traditional software contracts. It is necessary for public authorities to clauses relating to access to the program’s code in order to assure that, in the future, it will possible for the public body, or a new private partner, to adapt the software to new requirements.

Fair competence regulations may also work as an obstacle to establishing network access in certain places (e.g. rural areas) or through modern technologies (e.g. wi-

fi), as they offer no expectation of earning money for private partners while public authorities have neither the experience nor the funds to promote these initiatives. It is essential, then, to develop new business strategies combining public promotion and private partnership that are not based mainly on economic benefit or combined with other more profitable activities.

Finally, another relevant problem appears when several public agencies are interested in pooling resources for a common project. In this kind of situations, it is convenient to create a new organization (e.g. a consortium) with legal capacity in order to assume its own contractual obligations with a separate budget. As a consequence, a stronger capacity for negotiation with ICT companies and a higher coordination could be achieved.

6.5. What are the key management failings in moving to networked governance models?

This is one of the main legal problems related to interoperability. Since the EU has no concrete competences in this field, it may be addressed at the national level, bearing in mind some technical and administrative guidelines promoted at the European level but previously negotiated with national authorities. Although some Member States have established legal obligations in order to achieve technical compatibility, they should adopt clearer and stricter obligations if they have a direct competence in this field. Otherwise, they can use alternative methods, such as: offering financial aid to regional and local administrations for eGovernment issues only when there is a commitment to respect this exigency; or, when possible, trying to promote coordination and collaboration through other indirect means like technical support or developing common software, particularly at the local and regional levels. Creating a coordination structure where all the administrative levels are represented is also a desirable measure.

6.6. In what ways are policies relating to ICT procurement not technologically-neutral, and how is this affecting eGovernment take-up? How could technologically-neutral policies be better promoted?

National regulations on public procurement usually have no specific provisions on technological neutrality. Sometimes there is a clear obligation for public authorities not to refer to specific brands and, therefore, an indirect interdiction could be concluded in order to make eGovernment services available regardless the software used. Even more, as this kind of software is frequently designed by public administrations, this imprecise obligation is not suitable in these cases; therefore, more effective legal measures should be adopted. For instance, there is a clear obligation for public authorities and their private partners and contractors to use technical standards that make electronic services available regardless of the software used by citizens and companies.

Re-Use of Public Sector Information in eGovernment
Professor Cécile de Terwangne, CRID, University of Namur, Belgium

1. Description of the Area

Public sector information (PSI) is unique. As Herbert Burkert (1995) explains[272]: "Public sector information is not only the basis of public sector decision making, it also contributes essentially to the informational infrastructure of our societies. Its features are unique. It can – where necessary – be collected under a legal obligation on the information provider. It is associated with neutrality. It provides an 'informational backbone' to economic and social activities." The private sector has a great interest in this data as it may represent a unique source of certain information, while the public sector also has an interest in its own re-use of this data.

Public bodies gather details about citizens, business enterprises, land use, public decisions, vehicles, food, meteorology, health and most other sectors of society. Such public databases spread over different public services are being increasingly computerized, and eventually they may all be compatible with each other. This will make exchanges between databases technically possible, even if that may not be desirable or legally valid from some perspectives. Public sector information is therefore of great value, particularly in an electronic environment.

In EU Directive 2003/98/EC on the re-use of public sector information, usually referred to as the 'PSI Directive', 're-use' is defined as the use by persons or legal entities of documents held by public sector bodies for commercial or non-commercial purposes other than the initial purpose related to the public task for which the documents were produced. The exchange of documents between public sector bodies purely in pursuit of their public tasks does not constitute such re-use.

According to this Directive, such re-use aims to facilitate "the creation of Community-wide information products and services based on public sector documents, to enhance an effective cross-border use of public sector documents by private companies for added-value information products and services…". This should be allowed when enacted with total transparency and in a way that limits distortions of competition on the Community market – and everyone should know the conditions under which re-use can occur and whether competition rules are respected.

2. Why might this legal area be related to barriers to eGovernment?

Many eGovernment services depend on the re-use of information gathered or produced by public administrations, whether that re-use is proposed by the public sector itself or by interested private actors. Although the PSI Directive has an impact on eGovernment by tackling many related issues, it does not eliminate all obstacles concerning the re-use possibilities of PSI and the establishment of a pan-European public information market.[273] There are also important rights in this area, but these need to be re-evaluated if they are not to become obstacles to eGovernment.

[272] Burkert, H. (1995), *Public Sector Information: Some Implications for a European Information Infrastructure*, http://herbert-burkert.net/ARCHIV/1995-09-00-Vienna.pdf

[273] The MEPSIR study will bring results later in 2006 on the effects of the PSI Directive on re-use in EU Member States.

The following are key areas where potential obstacles relating to the re-use of public sector information are being encountered in the current European landscape:

1. The PSI Directive leaves to the Member States and their public bodies the determination of whether or not to allow the re-use of public sector information. Hence, there are no guarantees about the re-use of public sector information for citizens and businesses.

2. As the Directive bases the re-use system on the access regimes of the Member States, their implementation vary between Member States – and sometimes between different governance levels within a nation.

3. Exceptions exist to re-use permission, for example with some Freedom of Information (FOI) Acts prohibit certain kinds of re-use of the obtained information. In addition, data protection rules and/or intellectual property rights (IPR) conditions may prevent the re-use of some documents. Furthermore some documents are excluded from the scope of the PSI Directive (e.g. documents relating to public sector broadcasters and educational and cultural institutions, including museums.).

4. Competition rules that apply to the public sector must be considered in determining whether public bodies may themselves exploit public sector information.

5. Technical matters of significance to re-use effectiveness (e.g. a lack of common standards or formats; insufficiently clear information about ways to access public documents in Member States; and no common guidelines for storing such documents).

6. Difficulties arising from the need to cater for several languages.

7. A lack of clear harmonization regarding charges for the re-use of public documents.

3. What is the European context for this area, including legislation, policy statements and institutional arrangements relevant to this topic?

The main issues regarding the domain of public sector information were identified some years ago[274]. The Commission took its first steps on re-use in 1989 with the (not binding) Synergy Guidelines, which aimed to strengthen the position of the private sector in the European information market and limiting the role of the public sector bodies to the supply of raw data. In 1998, a second step resulted in the Green

[274] relevant publications inclue : Burkert (1995), *op.cit*; Y. Poullet, *Plaidoyer pour un ou des service(s) universel(s) d'informations publiques* , Conference of Stockholm, 1996; de Terwangne, C., *Droit à l'information et droit à la transparence. Vers une Europe de la connaissance?,* thèse de doctorat, Namur, 2000. See also events such as the Conference of Stockholm, "Access To Public Information: A Key To Commercial Growth And Electronic Democracy", 26 June 1996, http://europa.eu.int/ISPO/legal/stockholm/welcome.html and the INFOethics 2000 conference in Paris, 13-15 November 2000, http://webworld.unesco.org/infoethics2000/

Paper (European Commission 1995)[275] on public sector information. Thereafter, a proposal for a directive was issued that finally resulted in the PSI Directive.

As highlighted in its Recital 25, the objectives of the PSI Directive are primarily "to facilitate the creation of Community-wide information products and services based on public sector documents, to enhance an effective cross-border use of public sector documents by private companies for added-value information products and services and to limit distortions of competition on the Community market". It was also considered that this could not "be sufficiently achieved by the Member States and [would] therefore, in view of the intrinsic Community scope and impact of the said action, be better achieved at Community level".

On the basis of the Subsidiarity Principle of Article 5 of the Treaty, the Community took action in this domain, but it was limited by the principle of proportionality set out in the same article. However, this was not the only reason for the limited European harmonization in this domain. As Prins (2005) notes: "The remains of the political struggle and lobbying of different organizations are apparent when looking at the actual scope of the final directive. Here, the ambitious initiative to regulate the European information market is considerably mitigated. Various public sector documents that are in principle of high interest for the private sector are left outside the ambit of the regulatory regime."[276]

The re-use legal landscape in Europe is hence made of a patchwork of legal layers, which get entangled in each other. The upper (European) layer is built on the access to public information regimes allowed within the lower layers in Member States and the specific re-use rules applicable at national, regional, state or local levels.

4. What is the relationship of the Re-use of Public Sector Information to the seven barrier categories and associated research questions?

Of the seven barrier categories, three are important here: digital divides, poor coordination and workplace and organizational flexibility. Each are discussed below.

4.1. Poor Coordination (level of importance: significant)

As the PSI Directive leaves detailed regulation of the re-use of public sector information to the Member States and their public bodies, there is no overall guarantee in the EU regarding PSI re-use. At present, the commercial re-use is not allowed in all Member States. For example the current Federal Belgian FOI law of 11 April 1994 prohibits the commercial re-use of public sector information obtained through this Act: "The administrative documents obtained in the framework of the present law may not, for commercial purposes, be broadcasted, distributed, nor re-used"[277].

[275] European Commission (1998), 'Public Sector Information: A Key Resource for Europe', COM(1998)585.
[276] Prins, J.E.J. (2005), Commentary on Directive on the Re-use of Public Sector Information for "Concise Commentary on European IT Law, p.2
[277] A free translation of Article 10 of the federal Belgian law of 11 April 1994 on the publication of information by the administration. In Belgium, certain regulations at regional level severely punish as a penal offences the non-observance of a prohibition that is present at regional level.

The PSI Directive is therefore limited as a tool for harmonizing regulation of the re-use of public sector information, with no effect on the principle of whether re-use itself should be allowed. Despite a reliance on the access regimes of Member States, a common theme does exist to a certain extent through the principles laid down in Recommendation R(81) 19 of the Council of Europe. these have been taken as a model by many Member States (see Part 4, de Terwangne, C, 'Public Administration Transparency').

Some other rules regulating specific areas at national, regional or even local level may also have to be taken into account when addressing the question of re-use of PSI in order to develop eGovernment services or products. For example, obstacles may be encountered in the area of information about companies. In most European Member States, there is one central body that collects companies' information, as exemplified by the IT Consortium of Italian Chambers of Commerce, InfoCamere[278], in Italy and the Banque-Carrefour des Entreprises[279] (Crossroad-Bank of Enterprises) in Belgium. These bodies centralize detailed information on all the firms of the country, including items such as legal status, registration details and balance sheets. This offers a single location for anyone seeking information about a company, or a company wanting to license this information

Nevertheless, other European countries do not follow this centralized model. For instance, as Pira International (2000) explains: "In Germany companies do not register centrally but with their regional authorities. Hence companies wanting to exploit this information (such as directory publishers or credit information providers) need to contact all the individual regional authorities. In Greece the situation is even more difficult with no government department collecting companies information. This means that any organization wanting to publish information on Greek companies needs to get the information directly from each individual company."[280]

4.2. Workplace and organizational inflexibility (level of importance: somewhat significant)

4.2.1. Lack of a European culture of PSI re-use

In its brochure *Exploiting the Potential of Europe's Public Sector Information*, the European Commission (2004) sates: "The re-use of public sector information is a relatively new topic. With the Internet, the potential of this information as an economic asset has grown exponentially. This potential is, however, not widely identified within the public sector. There is at present no culture of systematically taking into account the possibility of re-use. It will take some time before such a culture develops throughout Europe"[281]. Although the adoption of the PSI Directive has begun to change this situation, this lack of a PSI re-use culture persists in Member States. For example, in the relatively under-developed market of

[278] http://www.infocamere.it
[279] http://kbo-bce-ps.mineco.fgov.be
[280] Examples cited in Pira International, *Commercial Exploitation of Europe's Public Sector Information*, Final Report, 30th October 2000, *e* Content – Spice Preparatory Action II, http://europa.eu.int/information_society/policy/psi/docs/pdfs/commercial_exploitation/commercial_final_report.pdf
[281] *Exploiting the Potential of Europe's Public Sector Information*, European Commission, Directorate General for the Information Society, Unit Information market (E4), May 2004, available at: http://europa.eu.int/information_society/policy/psi/library/index_en.htm#4.%20Brochure%20PSI 4

environmental information, obstacles are often caused by public suppliers who are not accustomed to locating appropriate information or negotiating with the private sector[282].

4.2.2. Exclusion of some documents

As previously indicated, some public sector documents are excluded from the scope of the PSI Directive, such as those for which third parties hold the IPR. In addition, Article 1(2)(a) of the PSI Directive determines that its regime is not applicable to documents that form part of an activity falling outside the scope of the public task of the public sector bodies. In applying the PSI Directive, it is therefore very important to determine what a public task is and is not.

A public task could be seen as a task that is directly related to the core activity of a public body, as opposed to an optional commercial product competing in the open market. But it is not always easy to identify directly what should be considered as related tasks (e.g. in order to offset overhead costs government trading funds may be employed to develop profitable commercial outlets for public administrations' services, which are often built around information provided as part of public task). However, this does not mean that everything produced by public bodies falls within the definition of a public task in relation to the PSI Directive.

The differences and uncertainties that exist between Member State regarding the basic definitions can create difficulties for EU citizens and enterprises in understanding the specific legal frameworks, for example knowing beforehand which re-use activities are worth introducing. Public administrations, on the other hand, may have difficulties in knowing exactly which documents – or part of documents – they are allowed to re-use.

4.2.3. Intellectual property rights

The PSI Directive has not solved the problem of divergences of national legal regimes regarding IPR or the absence of such rights for certain government documents. No existing intellectual property rights are affected by the PSI Directive.

The obstacles posed by IPR to accessing protected documents, such as providing an exemption to access rights) can be even more severe in relation to the re-use of public documents. For instance, although the holding of IPR on certain documents by public administrations may not prevent access to those documents, obtaining the right to re-use such documents could be much more difficult and more expensive than in the private sector. As a minimum, IPR requires obtaining the consent of the owner of the rights, and in many cases to pay to buy a licence to re-use the documents.

[282] Example cited in Pira international, *Commercial Exploitation of Europe's Public Sector Information*, Final Report, 30th October 2000, *e* Content – Spice Preparatory Action II, http://europa.eu.int/information_society/policy/psi/docs/pdfs/commercial_exploitation/commercial_final_report.pdf

4.2.4. Data protection

The data protection legal framework has an effect on the re-use of electronic public sector documents in that the PSI Directive cannot over-ride the protection of individuals with regard to the processing of personal data[283]. Thus, even if re-use is generally accepted in a Member State, it can be refused in a specific case on the basis of data protection rules. For instance, if a re-use purpose is not compatible with the initial administrative purpose for which the personal data has been collected, re-use cannot be accepted without the agreement of the person concerned.

Such a barrier to re-use and to the offer of certain kinds of eGovernment services and products is justified by the concern for protecting other important interests. The aim should therefore not be eliminate this, but to balance these interests with other factors affecting eGovernment outcomes.

4.2.5. Competition between public and private interests

Competition between public interests and private ones are real. Regarding electronic data, the difference between raw data and added-value data is small and public bodies are often tempted to exploit their information to gain revenue for themselves. Competition rules will not necessarily prevent public bodies from doing this, although they have an important influence on the entrance of some public or private actors in the re-use arena. For example, Pira International (2000) notes that "the main obstacle for companies working in the well-developed market of companies information may be potential competition from the public sector itself and the price it wants for the data"[284].

A first step already mentioned is to determine where the public bodies are acting within – or outside – the framework of their public mission. Another important point is the question of the application of the re-use legislation. For instance, what exactly is meant by the use "for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced?" Does this mean that the re-use legislation will be applicable as from the moment of the existence of a slight difference between the "re-use" purpose and the initial one, or should the purposes be completely different? Even when we are talking about an eGovernment service determined in the framework of the public mission of a public body, the re-use legislation can be applicable if we are outside the field of the initial purpose. However, this will not be easy to determine.

Public bodies must refrain from giving exclusivity rights to certain partners or to themselves regarding PSI re-use, and must also avoid cross-subsidiary of their commercial activities. In Sweden for instance, "there is an inadequate separation of commercial activities from public governance and public service functions of public agencies operating on a commercial scale."[285]

---

[283] Article 1(4) of the PSI Directive

[284] Example cited in Pira International, *Commercial Exploitation of Europe's Public Sector Information*, Final Report, 30th October 2000, *e* Content – Spice Preparatory Action II, http://europa.eu.int/information_society/policy/psi/docs/pdfs/commercial_exploitation/commercial_final_report.pdf

[285] Knut Rexed, Director General of the Swedish Statskontoret, 5th Meeting Public Sector Information Group, Luxembourg, 23 April 2004.

In the UK, the Office of Public Sector Information (OPSI)[286] is at the heart of information policy, setting standards and providing a practical framework of best practice for opening up and encouraging the re-use of public sector information. It offers a wide range of services to the public, the information industry, government and the wider public sector relating to finding, using, sharing and trading information. OPSI is a good example of the re-organization of services to meet the requirements of the PSI Directive. For instance it has:

> "improved dissemination of PSI and services to citizens and business; provides quick and easy access to data; established good public/private sector co-operation; created more effective, relevant and permanent links and thus enhanced inter-operability by improving the distribution of information across a variety of media, systems and different government departments; launched the online Click-Use Licenses which allow unrestricted use of government information. These standard licenses facilitate PSI exploitation by removing conflicts and simplifying negotiation between public bodies and private operators; publishes license terms and conditions, transparent pricing structure for the re-use and reply time; prohibits exclusive arrangements which hamper fair competition; has made digital format the primary form of dissemination; allows access to any pre-existing format; developed and adopted common standards and metadata; publishes electronic catalogues of accessible data resources and has created the Inforoute portal which is linked to decentralised assets lists; publishes how to complain or appeal if re-users feel that they have not been treated fairly."[287]

Comparisons of OPSI with other similar bodies illustrates the broader difficulties created by divergences between Member States on PSI re-use, particularly for the development of cross-border or pan-European information products or services. For instance, the French public service (SPDDI) providing law diffusion via the Internet has to make essential legal norms and case-law freely available for Internet users, for which the Légifrance website was created[288]. The re-use rules set out in the PSI Directive are met by both Légifrance (notably the transparency requirements) and OPSI. This illustrates how obstacles to re-use addressed by the Directive can be overcome.

However, the rules adopted to allow the re-use of published public sector information vary between different contexts. For example, Légifrance states that all the databases accessible through its website are protected under provisions of Title IV of Book III (Article L341-1) of the Code of Intellectual Property. This requires that every extraction or re-use of "quantitatively or qualitatively substantial parts of the content" of one of the databases supposes the previous conclusion of a licence to allow that re-use. The website explains what is perceived as a quantitatively substantial part or a qualitatively substantial part of the databases content. A user who does not intend to re-use such substantial parts may freely re-use almost everything contained in the French databases because most of these legal data are not covered by copyright

[286] Previously Her Majesty's Stationary Office (HMSO), See http://www.opsi.gov.uk/about/index.htm for more on OPSI.
[287] 'Practices of Exploitation of PSI', Deliverable related to WP2 Task 4 in the framework of the EPSINet Project, 25 August 2004, p. 14
[288] http://www.legifrance.gouv.fr

protection. OPSI policy, on the other hand, is different. Most UK legal material is covered by Crown copyright, which means a check has to be made of the items published on the OPSI website to determine whether a licence is needed for re-use or whether the person accessing the information falls into a listed exemption category.

4.3. Digital Divides (level of importance: somewhat significant)

Re-use of public sector information can be hindered by a lack of transparency about re-use possibilities and related practical issues that can benefit or disadvantage different sections of society, as discussed in the following subsections.

4.3.1. Charges

Article 6 of the PSI Directive has an imprecise reference to "a reasonable return of investment" when fixing charges for the re-use of public documents. This does not provide sufficient clarity as a harmonizing guideline.

However, the Directive imposes publicity conditions about the kind of information that needs to be provided to explain the terms under which PSI is available for re-use. For instance, despite the official implementation of the PSI Directive in Italy, InfoCamere does not comply with the Directive requirement as pricing conditions for re-using information contained in its data bases are not available on its website.[289] This indicates the current inadequacies of the Directive in addressing eGovernment barriers.

4.3.2. Re-usability of document formats

Offering public information for re-use purposes does not necessary imply that this information is easily re-useable. For this, documents need to be provided in formats that can be easily accessed by a wide range of potential users. At the same time, public services should not be expected to support unacceptably high new administrative and financial burdens in order to support any reformatting necessary to achieve this. Article 5 of the PSI Directive suggests a principle of delivery in electronic format "where possible and appropriate", with no obligation to create or adapt documents nor to provide extracts where this would involve disproportionate efforts. Reference is also made in Recital 13 to the need for conformity to open standards to ensure wide accessibility at least at a technical level.

4.3.3. Identifying the availability of documents

In a highly fragmented arena such as the public sector, it is difficult to know precisely what information is available for re-use. Article 9 of the PSI Directive refers to the need for practical arrangements to facilitate the search for available documents. An important organizational obstacle to eGovernment could arise if there is no clear, easily accessible and understood information for all citizens of all the Member States about, for instance, the way to obtain information, the availability of information and

[289] See http://www.infocamere.it for a detailed description of the InfoCamere case, see EPSINet, "Practices of Exploitation of PSI", Deliverable related to WP2 Task 4 in the framework of the EPSINet project, Florence, The Hague, 25 August 2004. The description presented in this document is still pertinent in May 2006.

the conditions under which such information can be accessed for re-use in every Member State. Without such information on re-use availability, regimes for cross-border or even national access and re-use regimes are likely to be ineffective.

The OPSI and French Légifrance services are examples of good practice in this respect, as they offer lists of information available for re-use together with simple 'click and use' methods to agree any necessary licence to enable appropriate re-use.

4.3.4. Language diversity

Due to the diversity of its Member States, a major obstacle to eGovernment developments in Europe can be the need to make available public documents in languages of other Member States, in ways that can be understood by citizens/businesses or public bodies of other Member States. As Prins (2005) observes: "Language diversity represents a challenge to the pan-European exploitation of public sector information. The costs involved in the translation of the raw material and the need for linguistic customization of the added-value end product is an additional difficulty that has to be overcome by information companies that want to step into this market."[290]

4.3.5. Common standards for storing public sector information

Another potential barrier is the lack of common principles and guidelines for storing PSI.[291]

An example of successful integration of data within one Member State is the MIDAS system in use in the Czech Republic, a public–private partnership that has operated since 2000 to provide a description and overview of existing data in the area of geographic information. It helps to co-ordinate data requirements, share data and remove duplication of efforts. The MIDAS free portal website[292] gives access to a large number of datasets drawn together from different sources within a common standard.

[290] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, eEurope 2002, *Creating a EU Framework for the Exploitation of Public Sector Information*, Brussels, 23.10.2001, COM (2001) 607 final
[291] *op. cit,* p. 16.
[292] http://www.cagi.cz/midas

PART 5: REFERENCES

Action Plan About Administrative Simplification, E-government and Readability 2005-2009, http://easi.wallonie.be

Alabau (2004), La Unión Europa y su Política Para el Desarrollo de la Administración Electróinca, Fundación Vodafone

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

Banisar, D. (2004), The FREEDOMINFO.ORG Global Survey – Freedom of Information and Access to Government Record Laws Around the World, May, http://www.freedominfo.org

Beers, T. A. L. (1996), 'National Secrecy Interests Versus Public Access', Conference of Stockholm on Access to Public Information, 27-28 June, p.1, http://europa.eu.int/ISPO/legal/stockholm/en/beers.html

Bergfeld, J. P., Kaspersen, H. W. K. and Lodder, A. R. Wob en ICT (2000), Onderzoek Naar de Gevolgen van Toepassing van Informatie- en Communicatietechnologie voor de Wet Openbaarheid van Bestuur. Amsterdam, , http://www.minbzk.nl/contents/pages/2134/evaluatie_wob_ict_11-00.pdf

Berkvens, J. M. A., van Esch and van Geest (2002) (eds), Automatiseringscontracten, Modellen voor de Praktijk (losbladig) (pp. 1-52). Deventer: Kluwer.

Biser Domain Report (2004), eGovernment – the Regional Dimension.

Building Archives of the Dutch municipality of Dordrecht: http://www.dordrecht.nl/pls/idad/prodEgemProductToon?F_PRODUCTID=999920021209131220

Bunyan, T. (2002), Secrecy and Openness in the European Union, Freedominfo.org, September, http://www.freedominfo.org/case/eustudy/index.html

Burkert, H., Public Sector Information: some implications for a European information infrastructure, http://herbert burkert.net/ARCHIV/1995-09-00-Vienna.pdf

Busch D (1998), 'Indirect Representation and the Lando Principles. An Analysis of Some Problem Areas from the Perspective of English Law', European Journal of Comparative Law, 2(3), December.

Business Access to State Information and Services', Website on the Irish Government's Basis, http://www.basis.ie/

Camp, L. J. (2003), Identity in Digital Government: A Research Report of the Digital Government Civic Scenario Workshop. Sponsored by National Science Foundation and the Kennedy School of Government.

Cap Gemini and TNO (2004), Does e-Government Pay Off?, November, http://europa.eu.int/idabc/en/document/3818/5666

Chantillon, G (2002), Responsabilité et Administration Electronique: Une Notion Revisitée. Report for the international colloquium: e-government for citizens organised by the University Paris-I Pantheon Sorbonne and the Conseil d'Etat, 21st and 22nd January 2002, in the Senate, http://dess-droit-Internet.univ-paris1.fr/bibliotheque/article.php3?id_article=277

Commission to the Council and the European Parliament (2006), 'Communication on the Interoperability for Pan-European eGovernment Services, COM (2006) 45 final, 13 February.

Commission to the European Parliament, the Council and the European Economic and Social Committee (2003), European Legislation: First Report on the

application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Brussels, 21 November, http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2003/com2003_0702en01.pdf

Conseil de l'Europe, Groupe des spécialistes sur l'accès aux informations officielles (DH-S-AC), 10ème réunion, Strasbourg, septembre 2003, Rapport, l'accès aux documents publics, http://www.coe.int

Council of Europe (1991), 'The introduction and use of personal identification numbers: the data protection issues; Council of Europe, Study of the Committee of experts on data protection (CJ-PD)', Strasbourg.

Council of Europe (2002), Replies to the Questionnaire on National Practices in Terms of Access to Official Documents, Strasbourg, November 2002, Document Sem-AC(2002)002 Bill to be found at http://www.coe.int/T/E/Human_rights/cddh/

Council of Europe (2005), "National Laws: Implementing the Data Protection Convention", August, http://www.coe.int

Data Protection Working Party (2003), Working Document on E-Government – Adopted on 8 May 2003; Article 29, 10593/02/EN, WP 73

De Terwangne, C. (2004), 'Accès à l'information et Organisations Internationales : le cas de l'Union Européenne', Ethique publique, revue internationale d'éthique sociale et gouvernementale, 6 (4), pp. 9-22

Delna, 'A Survey of Access to Information in Latvia', Transparency International, http://www.delna.lv/

Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Official Journal L 141, 04/06/1999, pp. 0020-0021 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

Directive 1999/93/EC of the European Parliament and of the council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 13, 19/01/ 2000, pp. 0012 -0020, Article 6.

Directive 2000/31/EC of the European Parliament and of the Council 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 L 178, 17/07/2000, pp. 0001-0015.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society Official Journal L 167, 22/06/2001, p. 10.

Directive 2001/84/EC of the European Parliament and of the Council of 27 December 2001 on the resale right for the benefit of the author of an original work of art, Official Journal L, 13/10/2001, p. 272.

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 (Directive on privacy and electronic communications) Official Journal L 201, 31/07/2002, pp. 0037-0047.

Directive 2003/98/EC on the Re-use of Public Sector Information of the European Parliament and of the Council of 17 November 2003, Official Journal L 345, 22/06/2001, p. 90

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, Official Journal 30/4/2004, L 157.
Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Official Journal L 210 , 07/08/1985 P. 0029 – 0033.
Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, Official Journal L 024, 27/01/1987.
Directive 91/250/EEC on the protection of computer programs of 14 May 1991, Official Journal L 122, 17/05/1991.
Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, Official Journal L 346, 27/11/1992.
Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Official Journal L 095, 21/04/1993, pp. 0029-0034.
Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, Official Journal L 248, 06/10/1993.
Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, Official Journal L 290, 24/11/1993.
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 L 281, 23/11/1995 pp. 0031-0050.
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, Official Journal L 077, 27/03/1996, pp. 0020-0028.
Directive 97/66/EC of 15 December 1997 of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal L. 024, 30/01/1998.
Dumortier, J. (2002), 'Directive 1999/93/EC on a Community Framework for Electronic Signatures', in A. R. Lodder and Kaspersen, H. W. K. (eds.), eDirectives: Guide to European Union Law on E-Commerce, The Hague/London/New York: Kluwer Law International.
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.
Dutch Copyright Act: Source: http://www.ivir.nl/legislation/nl/copyrightact.html
Dutton, W. (1999), Society on the Line, Oxford: Oxford University Press.
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, University of Oxford, http://www.oii.ox.ac.uk/research/publications.cfm
Dutton, W. H., Di Gennaro, C. and Hargrave, A. M. (2005), The Internet in Britain, Oxford: Oxford Internet Institute, University of Oxford http://www.oii.ox.ac.uk/research/oxis/oxis2005_report.pdf

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 (2005), 13-23.
eGov Stakeholder consultation (2005), http://europa.eu.int/information_society/activities/egovernment_research/index_en.hm
eGovernment Good Practice Framework website (http://www.egov-goodpractice.org)
EIPA (2005), 'Organizational Changes, Skills and the Role of Leadership', http://ec.europa.eu/idabc/en/document/4527/254
EPAN (2005): eAccessibility of public sector services in the European Union Report
European Commission (2002) Communication from the Commission 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), 'Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee. First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)', Brussels, 21.11.2003 COM (2003) 702 final.
European Commission (2003), Communication from the Commission to the Council and the European Parliament on Interoperability for Pan-European eGovernment Services
European Commission (2003), Comparative Analysis of Member States' and Candidates Countries' Legislation Concerning Access to Documents, http://www.europa.eu.int/comm/secretariat_general/sgc/acc_doc/docs/compa_en.pdf
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 (2004), Online Availability of Public Services: How is Europe Progressing?: Web-based Survey on Electronic Public Services, Report of the Fifth Measurement, http://europa.eu.int/information_society/soccul/egov/egov_benchmarking_2005.pdf
European Commission (2005), Communication on eAccessibility, http://europa.eu.int/information_society/policy/accessibility/com_ea_2005/index_en.htm
European Commission (2005), eAccessibility, 2005, COM (2005) 425, http://ec.europa.eu/information_society/policy/accessibility/com_ea_2005/a_documents/com_2005-0425-f_en_acte.pdf
European Commission (2005), Improved Effectiveness, Enhanced Interoperability and Synergies among European Databases in the area of Justice and Home Affairs, Communication from the Commission to the Council and the European Parliament, 24 November 2005, at http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0597en01.pdf
European Commission (2005), Overview of Member States' National Legislation Concerning Access to Documents, Document SG.B.2/VJ/CD D(2000) of 9 October 2000,

http://www.europa.eu.int/comm/secretariat_general/sgc/acc_doc/docs/apercu_en.pdf;
European Commission (2006), Application of the Rules on Protection of Personal Data by the Community Institutions and Bodies, March, http://www.europa.eu.int/comm/justice_home/fsj/privacy/eusupervisor/application-rules
European Commission (2006), Communication on Interoperability, COM(2006) 45 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, http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/egov_action_plan_en.pdf
European Commission (DG Information Society and Media) (2005), Study on Interoperability at Local and Regional Level.
European Commission (DG Information Society, e-Government Unit) (2004), User Satisfaction and Usage Survey of eGovernment Services.
European Commission (DG Information Society, e-Government Unit) (2005): CoBrA Recommendations to the eEurope Advisory Group
European Commission (Directorate General for Information Society and Media) (2003), Online Availability of Public Services: How is Europe Progressing?
European Commission (Directorate General for Information Society and Media) (2004), Online Availability of Public Services: How is Europe Progressing?
European Commission (IDA) (2002), 'Transborder eProcurement Study. Public eProcurement: Initiatives and Experiences: Borders and Enablers', http://ec.europa.eu/idabc/servlets/Doc?id=22188
European Commission (IDA) (2004), 'Linking up Europe: The Importance of Interoperability for eGovernment services', Commission Staff Working paper, IDA publications, January, http://europa.eu.int/idabc/en/document/2036/5583
European Commission (IDABC) (2004), Multi-channel Delivery of eGovernment Services.
European Commission (IDABC) (2004): European Interoperability Framework for Pan-European eGovernment Services.
European Commission (IDABC) (2005), eGovernment Observatory, eGovernment News, 13 July, Germany, Legal Aspects, http://www.europa.eu.int/idabc/en/document/4437/5864
European Commission (IDABC) (2005), eGovernment in the Member States of the European Union.
European Commission of Human Rights: Lindquist against Sweden (N° 10879/84); Lundvall against Sweden (N° 10473/83); and Kolzer against Sweden (N° 11762/85).
European Commission, 'Copyright and Neighbouring Rights' website, http://europa.eu.int/comm/internal_market/copyright/index_en.htm
European Court of Justice: Rechnungshof case, 20 May 2003 (the importance of the cumulative application of articles 6 and 7 of Directive 95/46/EC).
European Data protection Supervisor (2005) Second Annual Report 2005, , 19 April 2006, http://www.edps.eu.int/publications/annual_report/2005/AR_2005_EN.pdf
European Data Protection Supervisor (2005), Annual Report 2004, 18 March, www.edps.eu.int

European Data Protection Supervisor (2006), 'Comments on the Communication of the Commission on Interoperability of European Databases', 10 March, www.edps.eu.int
European Group on Tort Law (2005), Principles of European Tort Law, Text and Commentary, SpringerWienNewYork, http://www.egtl.org/
European Interoperability Framework for Pan-European eGovernment Services, version 1.0, November 2004, http://europa.eu.int/idabc/en/document/3473/5585
European Parliament (2000), 'Regulation (EC) 45/2001 of the European Parliament and of the Council 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, Official Journal of the European Communities L.8/1, 12/01/2001.
European Parliament (2001), '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. 145/43, 31/05/2001.
European Parliament (2004) Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of Intellectual Property Rights, Official Journal L 195, 2 June.
European Parliament (2006), 'Report from the Commission to the European Parliament and the Council on the operation of Directive 1999/93/EC on a Community framework for electronic signatures; COM (2006) 120 final, 15/03/2006
Feral, P-A. (2001), 'L'accès du Public aux Documents des Institutions Communautaires: la Consecration d'un Droit Fundamental de l'Union Européenne', Jurisclasseur, July, pp. 5 and f.
Gautier, P. Y. (2002), L'adaptation de Solutions de Droit Privé à l'administration Numérique.
Girot, C.: 'France', in E-Government and its implications for Administrative Law (2002)
Graafland-Essers, I. and Ettedgui, E. Benchmarking E-Government in Europe and the US, 2003, http://www.rand.org/publications/MR/MR1733/MR1733.pdf
Gross, T.: 'The legal framework for eGovernment' (2001)
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.
Harbour, M. and Gentry, S. (2005), 'Intellectual Property and the Challenge of Digital Technology', European Review of Political Technologies, December.
Heinderyckx, F. (2002), Assessing eGovernment Implementation Processes: A Pan-European Survey of Administrations Officials, in Traunmuller, R. and Lenk (eds). EGOV2002, LMCS, pp 111-115.
Institute for Prospective Technological Studies (2004), eGovernment in the EU in the Next Decade: The Vision and Key Challenges, http://europa.eu.int/idabc/en/document/3816/5666
Interview Anne-Marie Jorritsma, Nederlandse Zaken, wake up call voor de digitale overheid, Magazine Bestuursacademie Nederland.
Janssen, K. (2006), 'Hergebruik van Overheidsinformatie – Binnenkort ook bij u in de Winkel?', Privacy & Informatie, 69.
Johnssén, G. (2003), 'To Regulate Or Not To Regulate. E-government, Administrative Law and Change',http://www.skriver.nu/esociety/archives/gj2.PDF

Kranenborg, H. and Voermans, W. (2005), Access to Information in the European Union. A comparative Analysis of EC and Member State Legislation, Europa Law Publishing, Groningen.
Lefebvre, A., Poupaert, N. (2002), « Standardisation d'un guichet digital et échange de données en XML Analyse des aspects relatifs à la protection des données à caractère personnel »', SSTC-Privacy Project, CRID, University of Namur, October. http://www.droit.fundp.ac.be/crid/default.en.htm
Leitner, C. (2003), eGovernment in Europe: The State of Affairs, http://www.e-europeawards.org/view_extern.asp?id=4706
Lessig, L. (1999), Code and Other Laws of Cyberspace**:** How Will the Architecture of Cyberspace Change the Constitution?, Basic Books.
Lodder, A. R. and Kaspersen, H. W. K. (2002), eDirectives: Guide to European Union La won E-Commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection, The Hague/London/New York: Kluwer Law International.
Lueders, H. (2005), 'Intellectual Property Rights and eGovernment Interoperability in Europe', European Review of Political Technologies, December.
Marcou, G. (2002): 'Le régimen de l'acte administratif face à l'électronique'.
Margetts, H. (1999), Information Technology in Government: Britain and America, London: Routledge.
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.
National Electronic Commerce Coordinating Council, Identity Management. A White Paper Presented at the NECCC Annual Conference, December 4-6, 2002, New York, NY.
OECD (2003), Challenges for E-government Development, 5th Global Forum on Reinventing Government, Mexico City
OECD (2003), The eGovernment Imperative, http://Webdomino1.oecd.org/COMNET/PUM/egovproWeb.nsf/viewHtml/index/$FILE/E-Government%20Imperative%20Final().pdf
Open Society (2002), "Free Access to Information in the Czech Republic", August, http://www.otevrete.cz/index.php?id=142&akce=clanek
Papapavlou, G. (2000), 'Public Sector Initiatives in the European Union, Unesco Infoethics 2000', p. 7, http://Webworld.unesco.org/infoethics2000/
Prins, J. E. J. (2002): 'Taking Administrative Law into the Digital Era: Regulatory Initiatives in France, Germany, Norway and the United States', The Hague: TMC Asser Press; Norwell, MA : Distributed in North America by Kluwer Law International.
Remmen A. (2006). 'Images of eGovernment: Experiences from Digital North Denmark', in Hoff, J. (ed) 2006, Internet, Governance and Democracy, Denmark: Nias.
Riley, T. B. (2000), 'The Changing Shape of Information and the Role of Government', UNESCO Infoethics 2000, http://Webworld.unesco.org/infoethics2000/
RSA Laboratories, Frequently Asked Questions About Today's Cryptography, Version 4.1, http://www.rsasecurity.com/rsalabs/node.asp?id=2152
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, ETIS-LINK.
Seipel, P. (1996), 'Public Access to public sector-held information and dissemination policy – the Swedish experience', Conference of Stockholm on Access to Public Information, 27-28 June, http://europa.eu.int/ISPO/legal/stockholm/en/seipel.html
Statewatch's Observatory on public access to EU documents, http://www.statewatch.org/secret/observatory.htm
Staudenmayer, D. (2002), 'The Commission Communication on European Contract Law: What Future for European Contract Law?', European Review of Private Law 2, 249-260, Kluwer Law International.
UNDERSTAND (2005), Results Synopsis, http://www.understand-eu.net/
UNESCO (2002), 'Country Profiles of e-Governance', http://portal.unesco.org/ci/en/ev.php-URL_ID=5305&URL_DO=DO_TOPIC&URL_SECTION=201.html
United Nations (2003), World Public Sector Report: E-government at the Crossroads, New York, United Nations
Valero, J. (2004): Régimen jurídico de la e-Administración.
Välimäki, M. (2005), 'Software Interoperability and Intellectual Property Policy in Europe', European Review of Political Technologies, December.
von Bar, C, Lando, O. and Swann, S., Communication on European Contract Law: Joint Response of the Commission on European Contract Law and the Study Group on a European Civil Code, European Review of Private Law 2: 183 –248, 2002.
von Bar, C. and Drobnig, U. (2003), "Study on Property Law and Non-contractual Liability Law as they Relate to Contract Law" http://ec.europa.eu/comm/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/study.pdf
Yahiel, M. (2002), 'Des formulaires en lingne aux téleprocedures'. Administration électronique au service des citoyens P.31-37
Your Voice on eGovernment 2010 (2006), Online Public Consultation: Report, January, V 1.0.', http://europa.eu.int/idabc/servlets/Doc?id=24086.

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