JRC Scientific and Technical Reports

The Future of eGovernment

An exploration of ICT-driven models of eGovernment for the EU in 2020

(Executive Summary)

Authors: Valerie Frissen, Jeremy Millard, Noor Huijboom, Jonas Svava Iversen, Linda Kool, Bas Kotterink, Marc van Lieshout, Mildo van Staden, and Patrick van der Duin

Editors: David Osimo, Dieter Zinnbauer, and Annaflavia Bianchi

EUR 22897 EN - 2007

JRC EUROPEAN COMMISSION

ipts Institute for Prospective Technological Studies

Executive Summary

The Institute for Prospective Technology Studies (IPTS) has asked TNO and the Danish Technological Institute (DTI) to carry out a study which aims to provide European policy makers with strategic insights for future policy on eGovernment. The study aims to *analyse the potential of disruptive technology trends - and especially ICT - in providing challenges and opportunities for new models of eGovernment, public governance, public administration and democracy*. It builds on a vision on eGovernment for 2010,[1] which was developed by IPTS. The study acts within the political framework of the Lisbon objectives and the construction of the European Research Area.

The IPTS eGovernment vision for 2010 was developed as a result of a workshop in March 2004 in Seville. This vision points at the role of eGovernment as an *enabler* for better government, articulated around 'two pillars': the first being the pursuit of cost-effectiveness and efficiency, and the second the creation of public value. The approach in our study takes this vision as starting point and attempts to look further forward (to 2020). This study approaches the two pillars not as independent and equal pillars, but rather as 'means' and 'ends', with the interrelationship that this implies. This means that the *creation of public value* is the ultimate goal, and efficiency and effectiveness are only means to realise this higher end. Public value is related to the *outcomes* of eGovernment (on a broader economic, social and institutional level), and thus goes further than mere public sector or public service modernisation, which is the usual more narrow focus of eGovernment (research).[2]

The study also attempts to look beyond the current deployment and use of ICTs by governments and public administration, and particularly focuses on 'disruptive', or with a more positive connotation, 'promising' technologies: technologies which we assume will contribute to the *transformation* of (future) governmental tasks and activities. Promising technologies are those technologies which are both drivers and enablers of fundamental governmental change, needed to cope with future societal challenges. Transformative technologies may lead to a significant change in the existing establishment, open the gate to new players, lead to new institutional arrangements, change the value chain and relationship between actors and bring in new solutions to the complex problems that current governments are facing.

The general objective of the study can be broken down into the following more detailed goals and research steps:

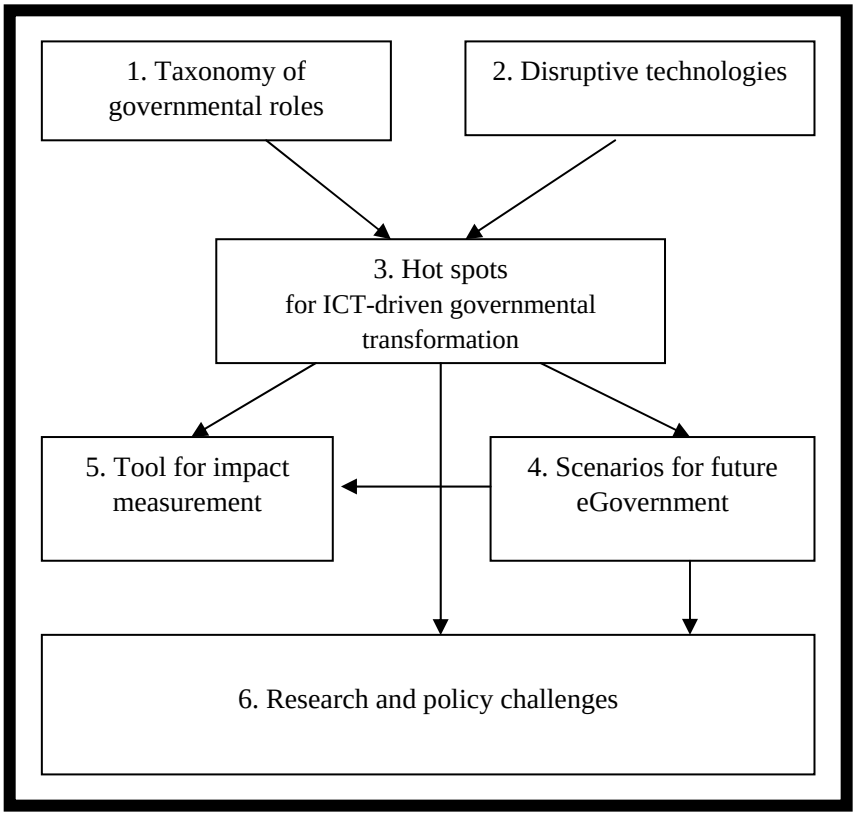
1. To build a taxonomy which describes the main existing and potential government activities, tasks and actions, which may be supported and enhanced by new applications and new use of ICT.
2. To identify, select and analyse those disruptive ICT technology trends which may have a transformative impact on future governmental tasks and roles.
3. To explore the potential innovation impact of new disruptive ICT technology for governmental roles and tasks (combination of 1 and 2).
4. To build – through a scenario exercise – the potential institutional, economic and social changes in the ways in which governance, public administration and democracy might be fulfilled.
5. To study the adaptability of the tools for measuring the impacts and changes envisaged within eGovernment activities, to the scenarios the evolution of technologies.
6. To draw research challenges and policy recommendations based on the hypotheses formulated by the study.

---

1 Eropean Commission (2004), "eGovernment in the EU in the next decade: vision and key challenges", C. Centeno, R. van Bavel and J.C. Burgelman, Final Draft version, August 2004, DG JRC, Institute for Prospective Technological Studies, Seville, Spain.

2 See Millard, J. 2003, ePublic services in Europe: past, present and future – research findings and new challenges, prepared for the European Commission's Institute for Prospective Technological Studies (IPTS), Seville, Spain, September 2003. Available from: http://www.cordis.lu/ist/about/socio-eco.htm and http://www.beepgovernment.org

Figure 1: Relation between project steps



Each of these goals has been the starting point for a specific study, which have been reported in six different research sub-reports containing most of the detailed and rich case-related material on which the analysis is based. The report you are reading now is the synthesis report, which brings together the main results and key conclusions of these different studies.

1.

The first step was to develop a taxonomy of key governmental roles, tasks and activities, which could be supported and enhanced by ICT. We have developed an overarching framework which reflects historical transformations in public values since the establishment of democratic constitutional states in Western countries. This framework[3] is depicted as a 'house of values', an edifice to which new storeys and rooms have been added and furnished over the course of centuries. Each storey of this house originated as a result of the major societal transitions that occurred during previous centuries. Whereas in the 18th century liberal values were central, in the 19th and the 20th centuries Western democracies evolved towards fully fledged welfare states. The dominant model on which these 20th-century welfare states were built is the Weberian bureaucracy of which functional division, centralisation and hierarchy are key characteristics. The characteristics of the Weberian bureaucracy, however, do not fit too well with ICT trends such as horizontalisation, decentralisation and the intertwining of activities and tasks. On the other hand, basic values of the foregoing centuries, such as integrity, legitimacy, accountability and equality remain of key importance for future government. Hence, a major challenge for governments is to reinvent models of government in such a way that they match current and future ICT trends and – at the same time – ensure existing and future values of good governance.

Each storey in our 'house of values' represents certain public values. The value or 'ends'-based framework is broken down at a highly detailed level into 'means', which refer to the roles, functions and activities of

[3] Inspired by among others: Bovens, M and Loos, E (2002) The digital constitutional state: democracy and law in the information society, *Information Polity*, Vol. 7, No. 4, 2002, pp. 185-197.

government that contribute to the realisation of these layered 'ends'. We have distinguished between the following values:

1. *Liberal values* (18th century): covering constitutional and subsidiarity structures; the legal framework: law, regulations and rules; law enforcement, defence and security; personal justice; and individual rights.

2. *Democratic values* (19th century): covering citizenship; democratic participation through representation; democratic participation through direct engagement; engaging private interests; and developing the plural society.

3. *Social values* (20th century): covering how needs for and responses to socio-economic support are determined; service design and production; service delivery; inclusion of all; environmental sustainability; place development and quality of life.

4. *Empowerment values* (21st century): covering how citizens, communities, groups and interests in society can be empowered to further their own as well as collective benefits; extending subsidiarity and reciprocity; governance coherence and balance; transparency and openness; ethics and accountability; trust; empowering the public sector as an individual actor; empowering the private sector; personalising services for individual users; and empowering the individual service user.

The fourth layer particularly represents the *future* 21st century model of public values and government roles and a stage of transformation, which is now – at the start of the 21st century – only rudimentarily beginning to take shape. Our first conclusion, therefore, is that a *shift towards empowerment* represents the most important transformation of governmental roles in the coming decades.

2.

In step 2 we have identified 'promising' technologies that may contribute to the enhancement of (future) governmental tasks and activities. Obviously, what can be seen as *promising* depends on what one wants to accomplish. As stated, from our perspective promising means 'creating public value' (in an efficient and effective way). Due to, among other factors, technological changes, the context in which government has to ensure these values has changed. In the past century, the industrial society has transformed into an information society. Traditional government, originally built on principles of the industrial society, is less and less able to face the complex demands and problems of the information society. The 'stove-pipe' architecture of public administration, but also a changing power balance in the political arena, hampers governments in fulfilling their tasks and in gaining citizens' trust.[4] In this light we consider promising technologies to be necessarily *transformative* technologies; technologies which enable the governmental scenery to change in such a way that societies are more able to cope with these emerging societal challenges. Transformative technologies may lead to a significant change in the existing establishment; open the gate to new players, lead to new institutional forms, change the value chain and relationship between actors and bring in new solutions to the complex problems that current governments are facing. In literature the notion 'transformative' – when related to technologies – is often called 'disruptive'.[5] [6]

Which technologies have this potential? One way of looking at this is to say that particularly the (large scale) deployment of technology is transformative.[7] However, not *all* technologies have a transformative

---

4 Fukuyama, F., The *Great Disruption, Human Nature and the Reconstruction of Social Order*, Touchstone, New York, 1999.

5 Christensen, C.M., *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, Boston, Massachusetts, 1997

6 In the FISTERA project disruptive technologies were defined as: *technological evolutions that lead to a disruption; this is a significant change in the scenario involving actors and the rules of the game* (WP2 Key European Technology Trajectories, First Report on Key European Technology Trajectories, 30 September 2003).

7 Carlota Perez, *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages*, New York: Edward Elgar, 2003.

impact when they are widely used; they must also have an intrinsic potential to become transformative. In our view, transformation can be enabled by high deployment of *existing* and by the introduction and use of *new* disruptive technologies. However, in the governmental realm, a lot of existing technologies with transformative potential are not fully deployed yet and thus have not been able to fulfil their innovative potential yet. Therefore, we expect that in the coming 10 to 15 years transformation will largely result from a process of adaptation and assimilation of existing technologies. Whereas in other sectors far-reaching deployment of existing technologies (such as social software and mobile devices) is or has already taken place, the exploitation of these technologies in government lags behind.

In short, in order to select technologies we have defined a transformative technology as a technology which:

- is broadly deployed,
- has an intrinsic transformative potential,
- has reached a certain stage of maturity and
- has the potential to stimulate disruption.

First we prepared a long list of technologies, with a group of technological experts from TNO, focusing on the disruptive potential of the technologies themselves. Then we clustered and reduced this long list focusing on the disruptive potential these technologies may have for governmental functions. This has led to the selection of the following key technologies:

- mobile devices (PDAs, wearable computers, MP3-players, mobile phones)
- intelligent agents (and robotics),
- sensors
- language processing technologies
- semantic technologies
- serious games
- RFID and biometrics,
- ICT infrastructures (WiFi, WiMAX, Broadband),
- web 2.0 technologies (social software)
- GRID

3.
The first two steps culminated in an analysis in which the roles and tasks of governments, as described in the taxonomy, were confronted with the characteristics of promising technologies. This has resulted in the identification of what we have labelled ‘hot spots’ of governmental transformation. The hot spots were selected using the following criteria:

(a) a combination of a mature technology with a governmental role

(b) which leads to governmental transformation

(c) within the majority of EU member states, and

(d) within the timeframe of 15 years.

Deployment and maturity of technologies were studied by gathering in-depth data on usage and usage barriers, market perspectives, application range and technological maturity (see also Appendix 1). The transformative and disruptive potential has been understood as a *complete change* of someone or something. (An example is the emergence of new balances of power, the adoption of new paradigms, the engagement of new stakeholders or institutional changes). The *significance* of a change determines whether a change is transformative or not; changes have to be large enough, general enough, and durable enough to affect considerably the character of (a setting of) organisations and to be called transformative. The four layers of governmental roles and responsibilities we identified in task 1 were used to assess the transformative impact of the technology, while justifying our assessment with literature, argumentation or

examples. This has resulted in the identification and clustering of combinations of roles and technologies into seven 'hot spots' (see the 'clouds' in table 7) of this report:

Transparency provoking change
ICTs are generally supposed to stimulate transparency. Promising technologies influence transparency in many ways:

- PDAs and mobile phones, which face a pervasive and still increasing popularity, enable ubiquitous access to all kind of information resources.
- Web technology, workflow and knowledge management systems stimulate the creation and dissemination of digital information.
- Technologies such as intelligent agents and semantic web support access to highly personalised information.
- Infrastructural technologies such as broadband, WiFi and WiMAX support high-speed and large-bandwidth data exchange.

Technology-driven increased transparency will have a wide range of impacts. Firstly, it will affect the power balance between governments and citizens (G2C) which will be based more on information symmetry and thus will increase the possibilities of citizens to exert effective control over their governments. Secondly, transparency will impact the relation between governmental agencies (G2G): it will stimulate and sometimes force governmental organisations to align their policies and procedures. It may increase competition between governmental agencies as well. Transparency may furthermore transform governmental culture, as it pushes governments towards opening up their traditionally quite closed and hierarchical organisation culture. Transparency may finally weaken the position of governments, as it will become more vulnerable to criminal activities.

Changing the accountability paradigm
In line with increased transparency, ICTs will also force governments to continuously account for their policy and decision making. Furthermore, and more fundamentally, new – more distributed – forms of accountability need to be developed. A broad range of technologies are expected to impact accountability in several ways:

- The decentralising character of web technology and social software will stimulate cross-boundary cooperation and the involvement of new stakeholders and therefore asks for new forms of accountability.
- Opportunities provided by technologies such as workflow, knowledge management systems and intelligent agents to computerise procedures and decision making may support a clear and unambiguous practice.
- The monitoring rationale of technologies such as workflow and knowledge management systems may increase the quantification of the accountability process.

The growing deployment of these technologies drives a trend towards networked models of government. This development will raise new questions on existing accountability constructions in EU Member states. Moreover, ICTs may strongly enforce accountability mechanisms. More and more accessible public sector information enables citizens to monitor government and to hold government practitioners and politicians accountable for their actions. Finally, ICTs may also provide governments with effective tools to fight corruption. Those EU member countries, which face a high level of administrative corruption, may profit from technologies, such as workflow systems, in order to combat corruption.

New forms of policing and law enforcement
Many of the promising ICTs we have distinguished increase the surveillance capabilities of governments, but also change the set of actors involved in law enforcement tasks. The large scale deployment of these technologies will affect the ability and the way in which the state exerts its role in the domains of law enforcement, defence and security.

- PDAs, digital cameras, etcetera, extend existing the overall surveillance capacity and enable improved direct intervention in cases perceived to conflict with the prevailing rule of law. They enable new stakeholders in matters of law enforcement and security which may lead to a decentralisation of (police) tasks.
- Mobile infrastructures such as WiMax, WiFi, and Broadband enable operating staff of public authorities to remain fully connected to the virtual infrastructures present within offices, adding to the self-reliance capacity of operating staff and thereby changing work processes and the work flow within public authorities.
- The decentralising character of social software enhances the opportunity for and capacity of individuals to actively engage in public affairs and influence decision making processes.
- Enabling technologies such as RFID and sensors provide the opportunity to create fully automated surveillance systems and thereby extend and improve existing surveillance and monitoring capacity.

As a result, both private organisations (such as security firms) and citizens will be increasingly involved in law enforcement tasks. Boundaries between stakeholders will become blurry. Law enforcement is increasingly pervasive (cameras, photos, etc.) and can be carried out more effectively (by using robots, RFID, etc). ICTs not only increase the possibilities to gather data but also to manipulate data (and thus evidence in court ruling).

Changing the privacy paradigm

The majority of the technologies we selected affect privacy. Most of the mentioned technologies are enablers of sophisticated and unnoticed data and information gathering. They enable the gathering of very detailed personal data, the construction of profiles that may be used to identify specific groups of people, as well as the tracking and tracing of people. This may take place in real time or in virtual space, on the basis of aggregated data. The role of technology in safeguarding the right to privacy is ambiguous: technologies are both a potential protector and an offender of privacy. On the one hand, government will be able to monitor individual citizens in greater detail, which increases possibilities of privacy infringements. On the other hand, ICTs may empower citizens to combine forces and to promote and protect their privacy interests. The sophistication of developing 'avoidance technologies' and technologies to remain anonymous in electronic communication practices (or in search techniques) will also increase.

New countervailing powers

Many of the promising technologies show a potential to open-up traditional forms of democratic involvement in governance, and to develop new ways to engage with individual citizens, communities, and advocacy/interest groups. These may thereby be empowered to become a new type of countervailing power to government. This can both supplement and change existing power structures in government itself, as well as in established power centres in the private and institutional sectors.

- Social software and social network tools are potentially revolutionary as they offer relatively cheap, easy to use and rapid means to informal as well as formal groups to organise themselves, develop common agendas, implement actions, and exert pressure on other power centres and stakeholders.
- This effect is even enhanced by the use of mobile devices, which enable the organisation and coordination of interest group activities in a *just in time, just in place* way.
- Similarly, the use of gaming, language processing and semantic technologies by groups can be transformative in the sense that new competences and new types of understanding and interpretation of information can be developed, which can underpin collective action.

The strengthening of bottom-up, often informal democratic involvement and the countervailing power which this engenders may cause a shift in the existing power balance between individuals, civil society, social movements and government. In terms of more far-reaching impacts, these technologies contribute to an on-going fragmentation of interests and thus of the system of political representation and a shift towards a more fluid, single issue or single event based politics with less institutional coherence. This is coined by

Bimber as 'accelerated pluralism'.[8] On the other hand the effect of this trend may also be that it will bind people more tightly together in social networks and thus enforce their position as countervailing power.

Networked government

This hot spot points to the trend that the horizontal, decentralized and location/time-independent character of technologies will increasingly drive networked, decentralized and multi-stakeholder models of government. The key technologies which drive and support this trend are:

- Infrastructural network technologies such as WiFi, WiMax, broadband and web technologies, which support the ubiquitous seamless connectivity and distribution of systems and services between stakeholders, including users.
- GRID, knowledge management and workflow technologies supporting the optimisation and interoperability of ICT resources amongst stakeholders by stimulating standardisation of languages, application, interfaces, etcetera, which could lead to organisational realignment, re-structuring and process innovation.
- The role of social software, social network tools, and technologies for decentralised service creation, all of which enhance bottom-up and personalised communication and information sharing. This promotes de-centralised and networked collaboration, participation and alternative service provision, which in turn stimulates new forms of organisation and changes to power balances.

When governments increasingly work together with other stakeholders, organisational and institutional arrangements and structures along the value chain have to change. A need for appropriate constitutional and political frameworks, legal and regulatory conditions, and mindsets and cultures will arise. The respective technologies can assist in transforming the organisational processes and resources of the actors and agencies involved, and, crucially, join them together to provide integrated and interoperable systems.

Intelligent and responsive government.

Here the focus is on the greater capacity of governments to collect, store, process and apply information. More and more useful information is being produced though knowledge-based, intelligent systems and is diffused in all kinds of societal networks, as well as across the public sector itself. This enables governments to design, produce and deliver higher quality and much better targeted and responsive services which are precisely tailored to meet the needs of specific individuals or groups. Promising technologies which are most relevant in this context are:

- Wearables, sensors, intelligent agents, robots, RFID, biometrics, GRID, and new tools for storage and retrieval which identify, collect and store information and make it available to government for intelligent processing.
- Knowledge management systems, semantic web, web technologies, plus PDAs and other mobile devices enable governments to convert information to intelligent knowledge and services, and thus to increase the responsiveness of government through new product and service innovations, and to deliver services to different types of users in new ways.

The identification, data collection, storage and processing technologies described above could develop into an *ambient technology* and thus an *ambient government environment*. Here, public systems and services will be everywhere, fully interoperable (in both technical and non-technical terms), and instantly and unobtrusively accessible through constant monitoring via network sensors and receptors of who is where, and what their needs are in changing situations. In such an ambient intelligent space, it will be even more important that governments ensure the reliability, resilience and pervasiveness of networks, Open source and open standards will be essential ingredients. Moreover, ensuring inclusion of all and the development of new forms of digital rights management will be important issues here.

---

[8] Bimber, B (1998) The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism, *Polity*, Fall 1998 issue, Vol. XXXI, Number 1, pp. 133-160.

We have concluded earlier that the shift towards empowerment represents the most important transformation of governmental roles in the coming decades. What we have seen by now is that ICT-related innovations are particularly important for driving this shift: each hot spot clearly shows signs of this empowerment trend: taken together the transformations described in the seven hot spots all cumulatively contribute to this shift. Different technologies support individuals in acquiring knowledge, organising themselves, to create, to produce and to deliver anytime and anywhere –. and thus: to be informed about government, to participate in public debates, to hold government accountable and to produce and deliver services that hitherto were collectively provided. It is particularly this empowerment trend which will affect the raison d'être of governments. In the seven hot spots we found the following strong indications for this shift:

- *Transparency*: as citizens and other stakeholders become better-informed and more aware of governmental activities they are better equipped (empowered) to directly address governments about their needs;
- *Accountability*: networked forms of governance enable citizens and other stakeholders to exert influence on the process of accountability but at the same time requires them to take responsibility for shared activities;
- *Policing and law enforcement*: both private and civic players are more and more enabled to take over policing and law enforcement roles, leading to co-production of roles or – in a more radical scenario – to a certain marginalisation of governments as law enforcers;
- *Privacy*: technologies are both a potential protector and offender of privacy; in the same vein, the role of government is ambiguous: intrusive in collecting more personal data; protective in offering protective measures; citizens become more empowered to keep control over personal data themselves;
- *Countervailing powers*: new forms of democratic participation contribute to enhancement of countervailing strategies; these forms are highly dynamic and volatile, highly pluralistic and fragmented and challenge the traditional mode of representative democracy;
- *Networked government*: by increased sharing of authority, bypassing of traditional hierarchies and vertical institutes, co-operation within government and with external stakeholders, external stakeholders are empowered and roles for government changes;
- *Intelligent government*: technological tools enable a shift towards a more responsive government, heading for service leadership, user-oriented character and context-awareness.

4.

Future models of government depend upon the way future trends will manifest themselves. Therefore, in the next step we have explored four scenarios for which the time horizon is the year 2020. The scenarios describe the consequences of promising ICT-developments for new eGovernment services and new eGovernment models in the wider context of related *social, economic, institutional and organisational* trends. Based on desk research we have made a list of trends with a high degree of uncertainty, but with a possible high impact on eGovernment. Sixty European experts (see Appendix) participated in a survey to select the trends with the expected highest uncertainty and largest impact. Their input was used to construct the axes of the scenarios. The scenarios vary on two highly uncertain factors that may have a large impact on future models of government: 'cultural diversity' and 'citizen involvement'. These two factors were selected by the experts as the most uncertain variables with the largest impact. When combining the extreme manifestations of these two factors (cultural homogeneity versus cultural heterogeneity and low versus high involvement of citizens), four images of government emerge in which we have taken the future activity of the hot spots into account in terms of their potential impacts in 2020. Experts were invited to engage in the creation of the scenarios in a two-stage process. In the first round, they were invited to comment on the generic descriptions of the contextual factors in each scenario. In the second, 'fine-tuning' stage, we asked them to further reflect on the scenarios which were then complemented with descriptions of the 7 hot spots described in earlier reports for this project. We asked them to comment on the following issues:

- In the Our Europe scenario, European culture in 2020 is coherent and homogeneous with a high degree of consensus on the future development of the European society. Democratic participation is high and citizens are overall quite involved in what their political representatives do: they are

well informed and able to express their needs. They critically follow their governments but in a constructive manner. Ambient government increasingly anticipates citizen needs. Government is focused on being efficient and effective in delivering personalised services. Because individuals and action groups, empowered with advanced personal media tools, can easily scrutinise and expose government operations, transparency and accountability have become the norm in and across government operations. A major challenge is to balance flexibility in projects and operations with this increased accountability. The potential for large-scale data mining by national governments and businesses is strongly regulated by EU privacy acts. eGovernment and eBusiness systems are designed around data sharing directives agreed at EU level. Intelligent devices comply with open EU standards to signal privacy incompatibilities when exchanging biodata. Governments receive extremely fine-grained, geographically-specific feedback on all their actions from all stakeholders and a kind of continuous referendum on key issues is emerging. To ensure concerted action there is a great need for common pools of knowledge and consistent and balanced interpretation across all spheres of government.

- In the We, the Market scenario, the private domain is by far the most important. People have come to rely on the structuring capacity of the market, which goes hand in hand with a transparent government that focuses on core tasks. Citizens are complacent and are hesitant to hold their governments responsible for their performance. Citizens have sacrificed their rights for data protection in exchange for job security in a volatile economic decade. Market parties manage this information to execute outsourced law enforcement tasks. Government's role is reduced to being a watchdog, as more and more key services are delivered through public/private partnerships. Many public services (health, public transport, education) have been 'outsourced' to the market as well with only a marginal role for public authorities. The market considers (personal) data as a commodity with a market value which skews the balance between privacy intrusion and market benefits. Privacy has become a trade-off mechanism between supply and demand. The market is in the lead when it comes to collecting, providing and exploiting the smart data needed to provide highly sophisticated and intelligent services and to create the ambient intelligent environment needed to support these. Companies use 'Google' business models, which can be characterised by smart ways of exploiting the collective intelligence present in societal networks. Democratic participation is low: people trust government. Checks and balances within the political system are primarily oriented towards enabling insight into costs and benefits. Government has outlawed the use of strong cryptography. The power of civil society groups to scrutinise business is curbed in new EU and national regulation. Businesses can sue activist groups if their image is tarnished.

- In the My Community scenario, the key characteristic of society is cultural, religious and political diversity. Units of governments cooperate in instant and horizontal networks which cause complex constructions of shared responsibilities. Thus accountability structures are very complex and opaque. Participants in governmental networks and citizens dispute responsibilities. Governments have substantially decentralised their tasks and activities; local communities and municipalities are the key actors in the public arena. Highly networked individuals and action groups mesh with business, which together dominate formerly traditional government domains. Governments influence and budgets are shrinking, and working in government has an increasingly bad image. ICTs have provided citizens with powerful tools to blow the whistle on government in terms of law enforcement and have empowered them to organise counter-surveillance and alternative forms of law enforcement. Successful online security firms and citizens' initiatives have taken over many traditional government functions in law enforcement. Citizens endorse an approach that prevents the ability to centralise the storage of personal data. As a result, service provision is fragmented and best accessible to those who can afford it. New cryptography technologies make it easy to scramble and disrupt aging ambient government technologies. The traditional model of representative democracy has been abolished and replaced by models based on deliberation, direct democracy and minority interests. Small collectives of loosely organised non-state actors muster power beyond the control of government. Their power depends on widely dispersed communities

that support them. These communities spring up and die out quickly making it difficult for government to develop any long term policies.

- The Me, myself and I scenario is characterised by low engagement and high – almost individualised – diversity. Low engagement drives a general attitude of minding your own business. There is little room for consensus building and a general distrust among all actors in society. Citizens care little about transparency and accountability. Surveillance and law enforcement are the key roles of government. For government, security is a perfect excuse for lack of accountability. Privacy is increasingly sacrificed in favour of security. Citizens are reluctant to reveal personal data to government. For some, personal data is a market commodity: depending on the services offered, citizens are willing to let their personal data be used for specific purposes (profiling, tracking, social network analysis and the like). "Clientelism" and one-to-one politics have become the corner stones of the democratic system. The role of governments in networks for public service provision has become quite marginal. In this scenario individual citizens use their personal budgets to organising key services, often through inside tracks with government. ICTs have enabled a high degree of personalisation of services which as a result are organised on a one-to-one basis in client-provider relationships between individual citizens and private companies or community providers. This fragmented services system makes good services hard to come by and expensive. Large sections of the aging European society have difficulties accessing key services such as dental care and affordable housing.

5.
Following the foregoing steps in the analysis, a future-oriented framework for measuring the benefits and impacts of eGovernment is presented. 'Future oriented' implies that this tool takes into account likely future transformations and new demands on eGovernment. In this case this means that the tool is specifically applied to the hot spots, as they represent our analysis of the key challenges for future eGovernment. This has been done in a concrete and pragmatic manner, providing a concrete indication of what could be measured when addressing the specific hot spots.

6.
Finally, and taking together the key points from all the research steps in the other research work, we have set out to identify the research challenges related with the new developments of eGovernment and to formulate policy recommendations. By research challenges we mean scientific blind spots; research themes or questions that will be relevant for future models of government and that are relatively new and underexposed. Policy recommendations are understood here as key challenges for future policy that derive from the identified research themes or from the trends or questions arising from the previous research tasks. Because the subjects of the five previous steps are rather divergent (vary from inventories of tasks and technologies to scenarios and impact measurement tools) and the interrelations between the tasks are manifold and versatile, we have chosen to identify the key research and policy challenges by using the hot spots as structuring element. We have first used the hot spots to identify the research challenges and have also taken into account here how relevant they are for the four scenarios.

As the seven hot spots show significant synergies, dependencies and overlap, and to bring a strong focus in the final concluding chapters, the hot spots have been further condensed into three relatively independent 'extreme' hot spots for ICT driven governmental transformation. For each 'extreme' hot spot we have first formulated the key research challenges (also based on input from experts taking part in a final validating workshop).

Extreme transparency
of government operations and functions on the one hand prompts close scrutiny of government accountability by citizens, business and civil groups. On the other hand, transparency of citizen activities raises serious issues of privacy. In both cases there are many new opportunities for due and undue police

surveillance and other law enforcement strategies. This has raised the following key issues for research (broken down into more detailed challenges in the chapter):

- How can the performance of more qualitative tasks of government be measured?
- What new forms of accountability (e.g. being responsible, giving account, holding accountable) fit the new models of networked government?
- What are good indicators to monitor the potential threat to privacy as a result of networked and intelligent government?

Fading boundaries
between government and its main counterparts in society are a signpost of the new ways in which government functions are being shaped. Coalitions of state and non-state actors (countervailing powers) play an increasing role in the implementation of government tasks. In research terms the following challenges come to the fore:

- What are the ways in which government can facilitate eParticipation and eDemocracy?

Enhanced intelligence
embodies the hot spots of an *intelligent* and *networked* government that exploits but also guards the many new sources of information gathered through granular interactive networks that now reach into every corner of society.

- What are the ways in which government can manage the overload of information as a result of 'ambient government'?

Finally, in the last and concluding chapter we have also used these extreme hot spots as the starting point for identifying key policy challenges and recommendations. But apart from these hot spot-related recommendations, we have also formulated some more general policy recommendations, which can be seen as pre-conditional for realising the ICT-driven models of eGovernment which we have described in this study;

General policy challenges
Political challenges

- Policy strategies and actions need to be based on an explicit value based *vision* on future eGovernment, which specifically takes into account the realisation of empowerment values.
- Future eGovernment models need to go beyond mere public service and public sector modernisation, and need to be based on a willingness to fundamentally change governmental operations, institutional arrangements and culture. In this sense the development of *incremental transition paths* is necessary, possibly based on different migration scenarios. This involves a need to look beyond short-term political agendas and implementation issues.
- The trend towards an increasingly networked eGovernment, will involve *cooperation and coordination at all levels of government and with new stakeholders and new intermediaries* at (and across) the local, regional, national and European level. This stresses the need for administrative and regulatory trans-European harmonisation to ensure 'interoperability' both at the organisational and the technological level.
- This harmonisation is also important to address the potential risks of an ambient, all knowing government, particularly to *ensure data protection (security and privacy) rights* of citizens and businesses.
- These kind of long-term and integrative transitional approaches require univocal *political commitment and strong leadership* with an impact on every level of government.

Technological challenges

- Ensure technological *interoperability and standardisation*.
- Governmental transformation requires back office re-organisation and one-stop shop approaches, which in turn require substantial *process and workflow redesign* that needs to be translated into

new *information architectures*. An extra challenge is that these new architectures need to be *flexible and open* in order to be sufficiently user-centred and dynamic.

- This also involves a stronger investment in technologies that enable *smart ways of cooperating and sharing or producing knowledge* ('collective intelligence', open source and open content, collaborative computing tools etc), among relevant stakeholders in this more networked environment.
- Ensure that networks and services are *accessible to all* both on the level of *infrastructures* as on the level of *services* and the necessary (user friendly) *interfaces* (usability).
- Stimulate the use of technologies which are designed to cope with potential *information overload* (e.g. use smart search engines, tagging technologies etcetera that are developed in social networks and in the context of user generated content)
- Reduce the *dependency on ICT-infrastructures* and related services or build in necessary safeguards (this requires an approach to cope with 'critical information infrastructures').

Socio-economic challenges

- The most important challenge will be to create the conditions for a *truly citizen- and user-centred* public service provision, which addresses empowerment values. This involves:
    - A highly developed awareness of citizens' and businesses' *needs* ('ambient government'): ambient government involves deep, personalised and pro- active knowledge about quite diverse user needs and the ability to translate these into highly diverse services, interfaces and access channels. It also point to the need to constantly monitor user needs, user experiences and user satisfaction;
    - Building *trust* through being transparent, responsive and accountable ('transparent government'); but trust also depends heavily on the ability to ensure security and privacy of personal data.
    - Diminishing the *regulatory barriers* for both citizens and businesses to be independent, self-organising and self-regulating ('light government').
    - Ensuring that public services are equally *accessible* to all European citizens and business ('inclusive government').
    - The latter also involves increasing the *awareness* of the potential benefits of eGovernment services. Currently, the level of deployment of eGovernment services is low, and there is strong evidence that lack of awareness of eGovernment services is the main barrier to take-up. Carefully targeted promotion and awareness campaigns should promote the overall benefits, calm the fears, and give general information about what is involved technically, where to find and how to use services. One aspect should be wider use of charters / codes of conduct / SLAs, etc.
- Another important challenge will be to create the *conditions for collaboration, coordination and knowledge sharing*, necessary for 'networked government'. Future government will increasingly be built on public-private partnerships and will involve new intermediaries in the public service delivery chain and in democratic processes. As a result, new governance structures and shared forms of accountability and transparency need to be designed. Furthermore, smart and efficient ways of sharing and producing knowledge between these different stakeholders will be increasingly important.

The more specific hot spot related challenges (described and elaborated in greater detail in the chapter) are:

Policy recommendations for 'extreme transparency'

- Transparency of governmental actions should be embedded in the design of ICT systems.
- Simplify regulations and procedures.
- Avoid redundant private data collection.
- New charters and codes should be developed on distributed electronic public sector transparency, accountability and privacy, where and how it applies and for whom.

- Promote and develop ICT-supported systems building on the collective intelligence of different stakeholders to stimulate and enhance networked models of policing and law enforcement.

Policy recommendations for 'fading boundaries'

- Engage citizens in the design of eGovernment applications in order to make them more citizen-centred.
- Develop charters and codes on public electronic access and input to the public sector decision- and policy-making process, feedback on that input including the results and reasons for use/non-use, and the expected behaviour and skills of civil servants and elected representatives in this context. This should include the rights and responsibilities of all stakeholders.

Policy recommendations for 'enhanced intelligence'

- Encourage cooperation and data sharing and cooperation between governmental departments and between government and other stakeholders (including citizens themselves).
- While encouraging cooperation between governmental departments/with other stakeholders (including the private sector and the civil society) in collecting, storing and exploiting data, at the same time develop policies on how these actors are allowed to use personally identifiable information. Policies need to be formulated in which the roles and responsibilities of government, civil society and business in the handling of potentially sensitive information are clearly articulated and in which shared standards for quality are articulated.

Government needs to be at the vanguard of semantic web and intelligent agent technologies to manage the flows of information that are coming their way.