iGovernment

SYNTHESIS OF WRR REPORT 86

WRR

SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY

iGovernment

The Netherlands Scientific Council for Government Policy (WRR) was established on a provisional basis in 1972. It was given a formal legal basis under the Act of Establishment of June, 30 1976. The present term of office runs up to December 31 2012.

According to the Act of Establishment, it is the Council's task to supply, in behalf of government policy, scientifically sound information on developments which may affect society in the long term, and to draw timely attention to likely anomalies and obstacles, to define major policy problems and to indicate policy alternatives.

The Council draws up its own programme of work, after consultation with the Prime Minister, who also takes cognisance of the cabinet's view on the proposed programme.

Lange Vijverberg 4-5
P.O. Box 20004
2500 EA 's-Gravenhage
Tel. + 31 (0)70 356 46 00
Fax + 31 (0)70 356 46 85
E-mail: info@wrr.nl
Internet: http://www.wrr.nl

WRR

SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY

iGovernment

SYNTHESIS OF WRR REPORT 86

Summary of WRR report 86 *iGovernment*, Corien Prins, Dennis Broeders, Henk Griffioen, Anne-Greet Keizer & Esther Keymolen (ISBN 978 90 8964 394 0), published by the Scientific Council for Government Policy (WRR) / Amsterdam University Press October 2011. The complete version is available on www.wrr.nl.

Design / layout: Studio Daniëls BV, The Hague
Illustrations: Silo-Strategie. Concepts. Design
Translation: Balance Amsterdam / Maastricht

CONTENTS

1 INTRODUCTION iGOVERNMENT

The core analysis in this report, entitled *iGovernment*, is based on the premise that – depending on the lens through which one looks – two variants of the 'digital government' can be observed. First there is the familiar eGovernment; we encounter this government in government policy documents and in the political and public debate. This is a government which thinks, discusses and acts on the basis of applications; a government which uses digitization primarily as a means of improving its service delivery and which believes in the power of technology for both policy and implementation. It is a government which has embraced the public transport ID chip card, the Reference Index of Juveniles at Risk and the Electronic Patient Dossier.

But we can also look through a different lens, and it is this other lens which the WRR uses in his report. Looking through this lens reveals a world where the emphasis is on information flows, rather than primarily on the technology that makes those information flows possible. If we look at the world behind all those individual applications and digitization efforts introduced in the drive towards eGovernment, we see revealed before us innumerable information flows – information flows which carve out a pathway for themselves within and between the various layers of government and which cut the across the boundaries of policy domains and also across the boundaries that separate the public and private sectors. This is the world of the information-Government.

In using the term iGovernment, this report is not only seeking to offer a new perspective, however. Possibly much more important is the WRR's desire to highlight the *actual existence* of a reality which is entirely different from the reality which currently figures on the political and administrative radar. The empirical analyses show that a burgeoning network of information flows is evolving, step by step, decision by decision, in the practical reality of every day: at central government level, at local level and at the level of implementation, and indisputably also at international and European level. iGovernment is more than a collection of decisions on individual applications and policy initiatives. In practice, it is found to be much more cohesive than we might imagine if we follow the familiar discussions about individual technologies and applications. Precisely because of this, the WRR wishes to use the perspective, or lens, of iGovernment to shed light on the fact that the Dutch government, despite a number of very modest initiatives, is almost completely unaware of the existence and implications of iGovernment, and as a consequence cannot evaluate developments within and outside government from that perspective, let alone steer them. This lack of political awareness of the existence of an iGovernment means that to all intents and purposes this new digital reality is unfettered by any 'natural' constraints. iGovernment has developed beneath the political radar, and if it remains there it will continue to grow unchecked. Mean-

while, however, iGovernment is ushering in far-reaching changes in the relationship between citizens and government. It is also creating new vulnerabilities, both for citizens themselves and for the government. In other words, although iGovernment has still barely appeared on the political and administrative radar, it has practical and very real implications for policy and implementation.

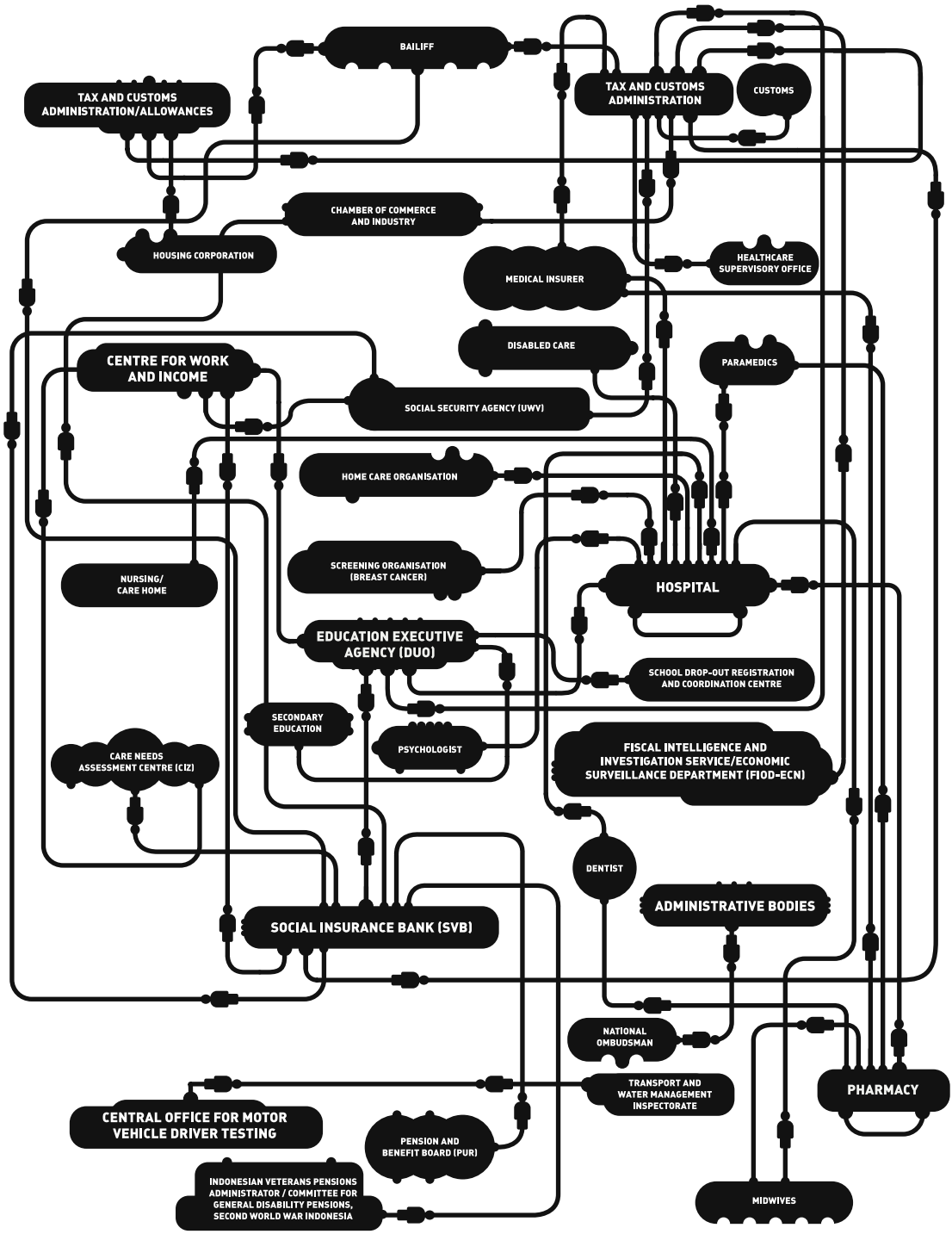
Reasoning from this starting point, this report argues in favour of making 'iGovernment self-awareness' a central and permanent objective for all layers of government. With this in mind, it provides a range of policy and institutional recommendations for making the necessary paradigm shift from eGovernment to iGovernment as smooth as possible.

1 THE IMPACT OF ICT ON SOCIETY AND GOVERNMENT

ICT has become part of the very fabric of government and it increasingly impacts on organisations, the professionals who work there, and their relationship with the public. All of the policy plans for eGovernment – which focus on internal operational issues, the provision of government services, and the technology itself – express massive trust in ICT as an instrument for making government more effective, client-friendly and accessible, for improving the quality of government, and for preparing government for the future. Increasingly, policymakers and politicians are turning eagerly to ICT to assist with the complex administrative work of government and to help them tackle urgent social issues such as terrorism, security, mobility, and the provision of good and affordable care. In addition to public services, other government tasks are rapidly being digitized.

Technology has very nearly become a matter of course in government, whether at the local, national or European level. Technology is 'rolled out', practices are 'streamlined' and services are 'updated'. The level of 'techno-trust' among politicians and policymakers can be seen in the hugely ambitious plans they have made for and with ict, not only in terms of the technology itself, but also with respect to actual policy. Currently popular policy themes – for example 'customisation' and proactive policy-making – would be unimaginable without the backdrop of digitization. In an effort to map out the future and anticipate what lies ahead, government is utilising and interlinking systems in such areas as security and care. For example, there is now a reference index in the Netherlands for children at risk; European immigration databases are meant to prevent more irregular migrants settling in the Netherlands; and special investigative databases and cross-border exchanges of passenger and bank details are helping to prevent new terrorist attacks worldwide. And it is not only national government that is planning new systems or calling for more and better information. Whole networks of interlinked systems and information processes are developing between implementing agencies and within local government. Globalization processes are also ensuring that information policy in

Data flows between governing and other organisations facilitated by the BSN



Source: www.burgerservicenummer.nl

the Netherlands is taking shape partly within the context of international as well as European applications and systems. There is also constant pressure at these levels to expand the systems' functions, to add more information categories, and to give a growing number of authorities access to the information stored there.

Politicians who wax lyrical about new applications as well as interlinked systems and information flows argue that these will increase security and improve effectiveness and efficiency. Combined with the problem-solving 'image' of ICT, the arguments they offer are more or less self-evident: in each case (a system, a link), these arguments appear to weigh more heavily in the equation than such ideals as transparency, privacy, freedom of choice, or accountability. Many policymakers who 'own' or advocate such applications tend to regard ICT as an instrument, and they assume – and regularly make a point of saying so – that it will not alter the primary process of government. They do not, or only barely, acknowledge or perceive the unintended but very real impact that digitization has on the way government operates, if only because the public in general has itself changed. Although the instrumental dimension of ICT is important, this attitude has led to a certain paucity, in the sense that that there is a virtual absence of any effective form of evaluation. Credible evaluations are rare and there are no sound standards for assessing applications. The debate continues to focus on the security of the technology (e.g. the public transport ID chip card) or the financial debacles (e.g. the various failed ICT projects).

The process of interlinking and sharing data runs parallel to the collapse of partitions between policy areas, between government organisations, and between the public and private sectors. Increasingly, such partitions are regarded – including by the public – as impediments to efficient and effective public administration. The popularity of data-sharing within supply chains and networks – something facilitated by unique ID numbers (the Citizen Service Number) and authenticated records – means that information can easily cross over traditional boundaries, even though the responsibility for the quality and reliability of that data have not evolved at the same pace. Information is disseminated, and it is used and processed by many different public authorities. Government bodies operating in widely diverging areas and with very different objectives are increasingly making use of the same 'pooled' information. But no one knows precisely who is responsible for the information (or its accuracy), and so people must allow for the possibility that 'their' information will come to lead a life of its own in public and private hands.

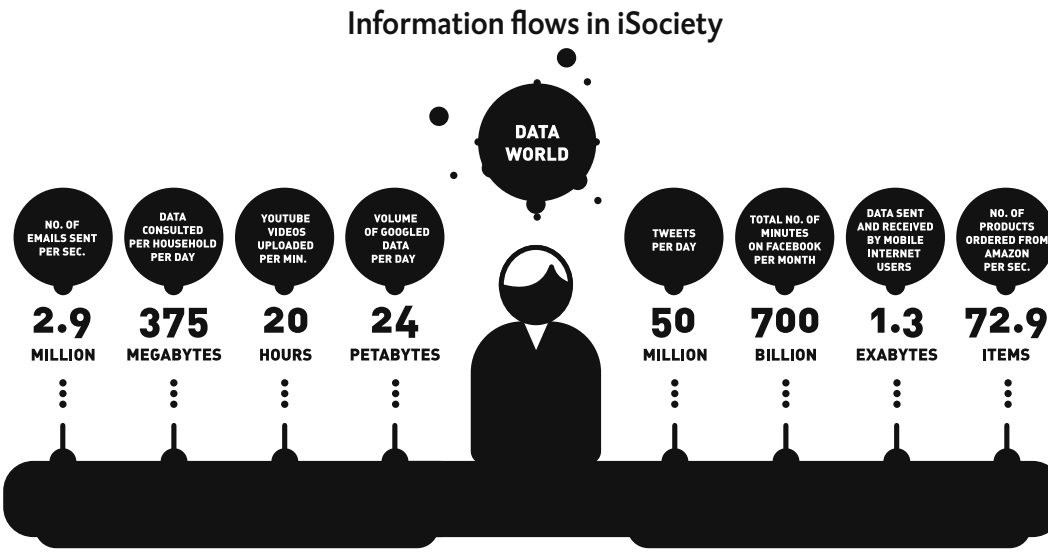
Politicians and policymakers propagate, discuss and assess all of the trends and developments described above, using a range of different rationales, ideas and normative viewpoints. The best-known of these are efficiency, effectiveness, security, privacy, and transparency. Ultimately, the form in which a new system or new link between information sources is cast is the outcome of a complex dynamic

relationship between all of these standards. That outcome concerns not only the technology – which is often the focus of the debate – but in particular its social, administrative and legal implications, which receive much less attention. To clarify this dynamic process and to offer some guidance when it comes to weighing up the various rationales at work, we have divided them into three categories: driving principles (such as security, effectiveness, and efficiency), underpinning principles (privacy and freedom of choice), and process-based principles (transparency and accountability). Driving principles are associated with government's 'drive' to utilise ICT in all kinds of different areas. They are closely bound up with notions of improvement and quality gains. Underpinning principles have to do with guaranteeing rights and freedoms, charting 'silent losses' as the process of digitization proceeds, and protecting the autonomy of the individual. They form a kind of counterbalance to the driving principles. Finally, process-based principles provide the procedural framework that makes a transparent and verifiable comparison between driving and underpinning principles possible.

2 iGOVERNMENT AS REALITY

The report shows that the nature of government is changing fundamentally, step by step, decision by decision, under the influence of digitization. A *de facto* practice has developed – virtually unnoticed – in which interrelated information flows dominate the character of government. These information flows therefore also determine the new possibilities open to the authorities and the public – as well as their dependencies and vulnerabilities. In everyday life , however, the overall idea of the 'information Government' – *iGovernment* – is virtually the last thing driving the way politicians and policymakers think and work: the vast majority of government initiatives relating to digitization and the information flows they generate are debated, evaluated and introduced in isolation. Individual initiatives are not – or scarcely ever – assessed on the basis of their impact or potential impact on government and society as a whole. The most significant omission is the failure or near-failure to view such initiatives within the context of the fast-expanding and rapidly diversifying information flows. Politicians and policymakers are not aware of iGovernment and, given the unremitting ascendency of ICT, that is certainly a problem.

The accumulation of ad hoc decisions about new technologies, the lack of awareness that iGovernment is on the rise, and the absence of any related discussion mean that when it comes to the development of iGovernment, 'the sky's the limit' – there appear, in effect, to be no limits. No one has restricted the dispersal of individual applications or the linking up of information flows, because no one has claimed stewardship of the whole. It no longer seems possible to set a frame of reference for collecting or linking information. The result is that information becomes contaminated, it is unclear who is responsible for information flows, and individuals, businesses and even government organisations become trapped and stifled in the tangle



Based on data provided by Cisco, Comscore, Mapreduce, Radicati Group, Twitter, YouTube.
Source: *Good Magazine*/Oliver Munday/IBM

of government data. Questions and concerns regarding the relationships between information flows and their implications are left unaddressed. As a result, not only people but also government itself are vulnerable. The debate among Dutch politicians and policymakers lacks a broader view of iGovernment and a meticulous and verifiable assessment of its driving pr, underpinning and process-based principles.

Although iGovernment is still developing and growing rapidly, and although it has scarcely made any impression on politicians and policymakers, it is already having a very real impact. At the same time, the lack of 'awareness' of the features of iGovernment means that this impact is scarcely taken into account in policymaking, and that politicians and policymakers do not realise sufficiently precisely *what* is developing, let alone *how* they can guide the development process in the right direction. If the Dutch government wants to steer the digitization process in the right direction while leaving enough scope for ICT-driven innovation, it will have to make the transition from eGovernment to iGovernment in thought, word and deed. Government's main challenge – and in fact, the challenge facing all tiers of public administration – is to understand that it has *already* become iGovernment, with all that that implies. Meeting this challenge will require it to shift perspective and develop an appropriate institutional framework. It must also, crucially, leave behind the narrow focus on individual applications, and turn instead to the idea of networked information management. The final requirement is that government must have an open-minded attitude toward trends and developments in the information society (iSociety). iGovernment cannot be structured in isolation. Its motto

must therefore be: 'Make sure we involve the iSociety in building an iGovernment that will last'.

3 ADMINISTRATIVE PRINCIPLES FOR iGOVERNMENT

Two issues are of vital importance in making the administrative transition to iGovernment. First of all, the scrupulous development of iGovernment is impossible unless we assess the driving, underpinning and process-based principles with an open mind. In addition, government must exercise particular caution, both in this assessment and in its policymaking and policy implementation, whenever the three processes of information handling noted in the report come into play. These processes – furnished with symbolic warning flags – are associated with a) the networking of information, b) the compiling and enhancing of information, and c) the pursuit of preventive policy based on information.
The three clusters of principles described in the report – driving, underpinning and process-based – should be well balanced at all decision-making levels. This is no mean task, given that a quasi-quantitative concept such as efficiency, a more normative concept like freedom of choice, and a process-based concept like accountability all clearly fall under different registers of analysis. Nevertheless, if iGovernment is to be evenly balanced, these three clusters of principles must also be thoroughly and properly assessed. They must be clarified, they must be verifiable, and publicly accountable. That does not happen nearly enough yet. Government must explain its rationale publicly at every level, from preparation and introduction of a specific application to the far-reaching diversification of processes and information flows that form the building blocks of iGovernment. It should do so not only at the national level, but also for assessments at the international and, specifically, at the European level. Clarifying the principles and making them as verifiable as possible would raise a number of issues and open them up for discussion. One such issue is the fact that politicians and policymakers are often irrationally optimistic about the potential of ICT. This is often why there impossible deadlines are set and why there are expensive ICT failures. Clarification would also show that spill-over and function creep are often quietly factored into the equation. Real iGovernment self-awareness requires politicians to take the expression 'A government forewarned is a government forearmed' seriously in the digital domain as well, and to apply this expression to implicit but foreseeable ICT trends. Government often anticipates the future in its policymaking, and it would be to its credit to do the same in its political assessments, openly and above board.

Secondly, the transition to iGovernment requires that government become much more aware of various features of information than is now the case. We are referring here to *processes* of information handling and use, specifically because such processes have a huge impact on the nature and reliability of the information that feeds iGovernment. We have therefore tagged three interrelated processes with

warning flags: when information is either part of or the result of these processes, government must pay strict attention to the quality of the information and consider who bears responsibility for it. The three processes that we have flagged in this way are:

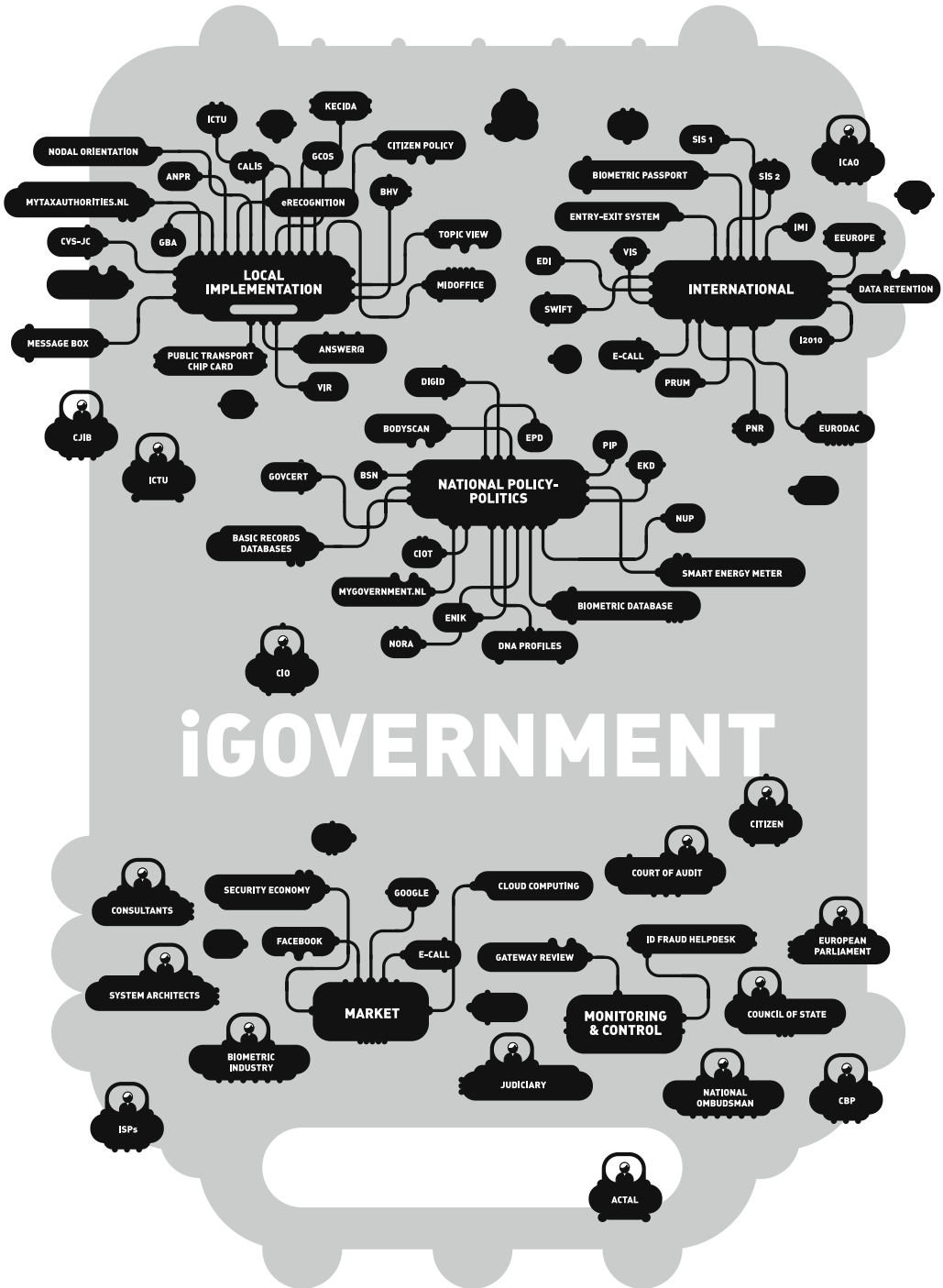
a The *networking* of information, i.e. shared use and management of information within a network of actors
b The *compiling* and *enhancing* of information, i.e. creating new information and profiles based on different sources in different contexts
c Pursuing *preventive* and proactive policy based on information, i.e. actively evaluating and intervening in society based on an information-driven risk calculation.

These three information processes, which are the core of iGovernment, enable it to fine-tune and customise policy, obtain a comprehensive picture of the public and of the policy issues, and take proactive action where needed. At the same time, they are processes that themselves have an impact on information: they influence its nature, reliability, recognisability, contextuality and traceability. It is important to realise – much more so than is now the case – that it is precisely these three processes that are having the biggest impact on (a) the quality of information *content* and (b) the demands made on the *organisational* context of information flows. The quality and vulnerability of information and information processes therefore require constant, proactive vigilance throughout all branches of national government. We must also have a much greater degree of openness and transparency, so that we can help people understand what information is being collected on them and assist them in correcting it where necessary. Right now, people are almost powerless to correct errors in personal information within the vast iGovernment information networks – errors that sometimes have huge repercussions. Finally, iGovernment's 'memory' demands particular attention. Both the importance of 'forgetting' – people should not be judged eternally on the information that government has stored about them – and of saving and archiving require a radical cultural transition and a firmly grounded strategy.

4 LIMITS TO THE GROWTH OF iGOVERNMENT

When iGovernment is not self-aware, its natural tendency will be to continue expanding. After all, only self-awareness will induce it to set limits to its own growth. The scrupulous development of iGovernment also means being prepared to set limits to it. Although the report does not define such limits – in essence, that is a political matter – it does indicate where those limits might be found. In the first place, the combined processes of assessing principles and being alert to warning flags force us to consider the limits of iGovernment. Other reasons to set limits may include the mixing of service, care and control, and the diffuse boundaries between public and private information flows. What is also of huge importance is the fact that the

iGovernment depicted



Internet has created an entirely new information environment, one from which iGovernment cannot withdraw and within which it is obliged to function. The relationship to this 'world outside' also makes it very important to set well-argued limits.

5 AN INSTITUTIONAL AGENDA FOR THE TRANSITION TO iGOVERNMENT

Prudent efforts to build iGovernment require changes not only in policy but also at the institutional level. A government that has taken on another guise in the digital sense must also make the necessary organisational changes. When government is linked up in terms of its information flows, the accountability structure must fit in with this new reality and operate with the necessary efficiency. 'iGovernment self-awareness' is not just a status to be enjoyed, but rather an ongoing challenge that must ultimately be ingrained in every tier of government. In the short term, however, central government will have to foster that self-awareness. Fleshing out the targets for iGovernment will therefore require an institutional transformation that assigns and embeds three functions within government:

a The *strategic function*, i.e. guaranteeing the well-considered, ongoing development of iGovernment
b The *societal function*, i.e. making iGovernment more transparent for citizens and improving its accountability *vis-à-vis* individuals who become entangled in information networks
c The *operational function*, i.e. improving the well-reasoned alignment between policy, implementation, technology, information flows and networks. Also, improving the commissioning practices of government.

These three functions constitute the absolute minimum requirements for shaping iGovernment self-awareness and acting on the implications of the new reality. It is no easy matter to map out the institutions associated with these three functions properly, but it is important that these functions are actually entrusted to organisations. The institutional transformation as such is much more important than the precise designations for the institutions proposed in this volume. At the strategic level, we propose a standing committee for iGovernment that investigates and assesses digitization processes in the light of iGovernment as a whole, and that reports to Parliament. At the societal level, we propose setting up an iPlatform in order to concentrate and increase the transparency of iGovernment *vis-à-vis* citizens. Accountability can be entrusted to an iAuthority, responsible for dealing with any problems that citizens encounter with iGovernment (and given the power to take binding decisions). Finally, it is of vital importance at the operational level to ensure professionalism in commissioning practices and to prioritise not technical expertise, but expertise at the interface of technology and policy.

In essence, this publication is about government taking responsibility for the way it uses ICT. But government naturally also has a role to play in the information society. In addition to being accountable for iGovernment, government is responsible to some extent for the way the iSociety functions. What aspects of the information society should government be concerned about, and when should it intervene (and how)? The general public and businesses move ahead, inspired by the promise of new technologies and profits. When this development is not offset against underpinning principles and balanced against the outcome of processbased principles that make information flows transparent for the public – and, if necessary, open to criticism – then those involved iGovernment should at the very least ask whether the time has not come to take action.

II RECOMMENDATIONS: WORKING ON iGOVERNMENT

Government must become aware that it has developed from an eGovernment into an iGovernment. That awareness is essential if it hopes to meet the challenges of unremitting digitization and to use digitization to exploit the benefits of innovation. A rationale based on iGovernment self-awareness will require government to look beyond technology and individual applications and shift its view to a broader perspective on information. That broader perspective means focusing on the information flows that result from the many different applications and the connections between them. In particular, it also means considering the consequences for society and policymaking of the ongoing expansion and specific dynamic of iGovernment.

It is tempting to assign the task of accomplishing the necessary transformation and related measures to a particular ministry, organisation or official, i.e. to assign responsibility to a single entity or person with an overall view of iGovernment. That is largely impractical, however, given the scale, complexity and multifarious implications of ICT for the relationship between government and the citizen. The report cannot provide a comprehensive strategy or blueprint for arriving at an evenly balanced development of iGovernment, nor do the authors expect 'government', understood as a single entity, to do so. iGovernment self-awareness and the consequences of that awareness will have to sink down through the many levels and institutions that make up government, i.e. the ministries, agencies, local authorities, police, regulatory bodies, citizens, and – last but not least – politicians. iGovernment has evolved in many different places within government, and awareness of its consequences will have to do so as well. Be that as it may, it is naturally also true that, as George Orwell put it, "all animals are equal, but some animals are more equal than others." The current chapter will suggest a number of organisations to take on the responsibility of promoting this awareness and guiding the evolution of iGovernment in the right direction. These 'duties' should be viewed as the organisational side of an agenda of government transformation. The transition from eGovernment to iGovernment requires a paradigm shift that can be detected in the real-life developments described in previous chapters, but that must now, crucially, be embedded in the institutions of government and their thinking. That transformative *agenda* is much more important than any specific suggestions relating to the institutions themselves. Many roads lead to Rome, but government cannot afford never to arrive in Rome at all.

The first three sections of this chapter make a number of normative and procedural recommendations. Paragraph 1 begins by offering recommendations for the tripartite division into driving, underpinning and process-based principles presented earlier in the report, which have played such an important role in our empirical analysis. Based on that analysis, paragraph 2 describes three properties of informa-

tion that should serve as warning flags for self-aware iGovernment. These are not *categories* of information, but *features* of information processes that require special guarantees both for government itself and for its relationship with the citizen. Such guarantees form the basis for the two recommendations made in paragraph 2; these, in turn, provide a basis for reflecting on the limits of iGovernment, as recommended in subparagraph 2.3. Finally, paragraphs 3 and 4 describe the components of an institutional framework for embedding 'iGovernment selfawareness'.

1 WEIGHING UP THE DRIVING, UNDERPINNING AND PROCESS-BASED PRINCIPLES

As experience has shown, the dynamic relationship between the driving principles (notably, effectiveness/efficiency and security) and the underpinning principles (notably, privacy and freedom of choice) is a defining factor in the evolution of iGovernment. In addition, process-based notions such as transparency and accountability point out the difficulties of creating a normative and institutional context for the development of iGovernment, as well as the opportunities that such a context creates. When put on the spot, every official – whether policymaker, politician or public servant – will attest to the importance of *all* these principles. After all, they appeal to common sense, responsibility, fundamental values, and due care. No one opposes security or privacy, for example, the two concepts that are most often played off against one another. And no one will deny that these principles should be weighed up carefully against one another. The decisionmaking process must, after all, be evenly balanced; decision-makers must look at all sides of an issue. When it comes to the theoretical foundations, then, there is general consensus. The everyday reality of government is often very different, however, as Part II of the report has made clear. As noted in previous chapters, ICT should be seen as a political choice and, as such, as more than a purely instrumental solution to a problem. When all is said and done, politics is strife. In the real world in which iGovernment is evolving, the process whereby politicians and policymakers weigh up the various principles is a less evenly balanced and public affair, as a rule, than theory might lead us to believe. There are a number of reasons why that is so: first of all, the principles are seldom discussed explicitly and openly; secondly, the principles are dissimilar and therefore difficult to pin down and weigh up against one another; and finally, a skewed presentation of issues can be advantageous in politics and policymaking. We look in detail at these reasons below and propose two recommendations for making the rationale and the debate on iGovernment more open, explicit and realistic with respect to the associated principles.

The three clusters of principles described in this volume – driving, underpinning and process-based – should be well balanced at all decision-making levels. That is no mean task, given that a quasi-quantitative concept such as efficiency, a more normative concept such as freedom of choice, and a process-based concept such

as accountability all clearly fall under different registers of analysis. Furthermore, driving principles such as efficiency and security need very little encouragement to claim the limelight, as experience has shown.

That is often otherwise when it comes to the underpinning principles. These are grounded in civil liberties and individual autonomy and are enshrined in the principles of privacy and freedom of choice. Although the concept of freedom seems fundamental and absolute, such notions are in fact much more pliable in everyday life than the arguments that weigh in on the other side of the scale, i.e. efficiency and security. The argument that we must embed such principles institutionally is often prompted by the fear that individual interests will be harmed; that fear tends to lose out when weighed up against the perceived interests of the collective. In other words, the privacy of an individual is often not as important as the safety and security of the collective. Regulatory and judicial reviews virtually always focus on whether the infringement of a fundamental right is proportional. Valuable as the notion of proportionality may be, it runs into the difficult that there is really no common unit of measure or currency that allows us to make a quasi-mathematical comparison between dissimilar clusters of principles (driving versus underpinning). The problem with squeezing such a comparison into one particular straightjacket – for example a cost-benefit analysis – is that the arguments (and the language) of effectiveness/efficiency tend to prevail.

In everyday life , finding the right balance between the driving and underpinning principles of iGovernment often depends on the degree to which the intermediary, process-based principles of accountability and transparency have been put into effect. Without a sound application of these principles, no assessment is guaranteed a solid foundation. The principles of accountability and transparency must ensure the validity of the process by which iGovernment develops. Together, these principles require the implicit choices made by government to be made explicit: clear, comprehensible, open to discussion, and susceptible to objection. In fact, the only credible way to weigh up the various principles against one another in this context is by means of argumentation. In order to give such argumentation free rein, government must explain its rationale publicly at every level. One of the most important agenda items for iGovernment is that government must be required to explain, explicitly, how it weighs up the principles involved (a process that is unavoidable). That process must be laid bare at all levels, from the preparation and introduction of a specific application to the comprehensive diversification of processes and information flows that form the building blocks of iGovernment. Government must explain its rationale not only at the national level, but also with respect to the decisions it takes at the international and, specifically, at the European level. That requires the Dutch Government to clarify well in advance what rationale it intends to bring to the European conference table and what results, in terms of that rationale, it hopes to take back home. This brings us to our first recommendation.

An evenly balanced development of iGovernment requires the driving, underpinning and process-based principles to be properly weighed up against one another in a manner that is clear, verifiable and can be publicly accounted for.

There is an urgent need for government to weigh up the various principles comprehensively and publicly, as doing so will help it avoid the undesirable consequences that may ensue from a unilateral approach to iGovernment. Ultimately, the single-minded pursuit of one principle only (whether it be security, privacy, transparency, or any other) means that iGovernment will gradually – application by application and link by link – take on an extreme, impractical and vulnerable form. It is therefore important to keep an eye out for signs and warnings that one or more of these principles are set to stifle the rest. After all, society can have too little of a specific principle – but too much as well. The potential danger of domination applies to *all* principles, especially when taken to extremes: driving principles such as effectiveness/efficiency become economic reductionism; underpinning principles such as freedom of choice become choice overload; and even a process-based principle such as accountability can result in excessive mistrust and litigiousness when applied unilaterally. But even the 'midfield' – between the two extremes – requires a proper balance. Too much emphasis on security may soon be at the expense of privacy and transparency. Too much emphasis on privacy, on the other hand, may be at the expense of transparency and accountability, as accountability always requires a certain degree of openness. All too often, initiatives have gone ahead without a genuine, meticulous and verifiable comparison between these dissimilar principles. The comparisons that have been made – for example as explained in parliamentary documents – are often fragmented and/or superficial.

That is not only due to the conceptual difficulty of reaching a credible balance, of course. The principles must be weighed up at different moments, at a variety of different levels, and in the many different processes and procedures that together result in iGovernment: in a parliamentary debate about a new application; when describing the work contracted out to an applications designer; when deciding to link files or connect new organisations to a network; and in the rulings and opinions of the courts, regulatory bodies, and citizens regarding new developments and decisions. There is much at stake in each of these situations, and one can at times witness a tendency to allow a single principle to overrule the others simply in order to be done with a dispute or avoid a dispute in advance. It has happened numerous times in the course of iGovernment's evolution that plans for a new application were unveiled in a way closely resembling a marketing campaign. At times, 'techno-trust' is not really trust *per se*; it is really more of a political sales pitch. A little less hocus-pocus with terms such as effectiveness/efficiency and security would be advisable. But realistic and verifiable arguments and comparisons are also lacking at the other end of the spectrum, for the underpinning principles of privacy and freedom of choice. If something has to be sacrificed at that end (and that is often enough

the case), then the 'loss' should be acknowledged and communicated as such. In other words, although in most cases it is not clear in advance what the 'right' balance is between the driving and underpinning principles, the debate on this question is in sore need of improvement.

Discussions as to how iGovernment is to evolve further and the role that the principles should play in its development must be more solidly grounded in reality. So far, neither those who emphasise the opportunities nor those who emphasise the dangers have argued their case entirely credibly. The process-based principles of transparency and accountability can play an important role in this respect. A sound and credible process-based framework for iGovernment can help ground the discussions about the direction that should be taken in reality. The arguments relating to the underpinning principles must also be made explicit and as verifiable as possible. It particular, it would be more realistic at this end of the spectrum to cease regarding privacy and freedom of choice as all-or-nothing principles. Sometimes it is in fact necessary to sacrifice a degree of privacy or freedom of choice, provided that the sacrifice is made clear and there is good reason for it. Government should not, after all, pass up every opportunity to use modern technology and scientifically sound methods of risk assessment, diagnosis and intervention to protect human lives (Buruma 2011). Too much privacy may mean that the authorities never become aware of a child at risk; too much freedom of choice in a complex situation may leave citizens empty-handed after all.

Clarifying the driving principles and making them as verifiable as possible would in turn raise two issues and open them up for discussion. The first of these is the often unjustified optimism among politicians and policymakers about what ICT can do, as the cases cited in previous chapters and in many other studies have shown. Although optimism often drives innovation, in the Netherlands it has led to ad hoc projects, impossible deadlines, and expensive ICT failures. The second issue is that 'spill over' and 'function creep' are often quietly calculated into the equation from the very start of project. Officially, politicians distance themselves from such 'fiddling' and reject it in their discussions and debates, but they are in fact fully aware that the future is likely to bring precisely the thing that the Government is officially ruling out at an earlier point in time. The formal argument then is that political responsibility only extends to the proposal at hand, and not to the possibilities that the proposal holds out (implicitly, but without requiring too much imagination). When iGovernment consists of a chain of such isolated decisions, reasoning of the 'after us, the Deluge' kind is simply untenable. Real iGovernment self-awareness requires politicians to take the expression 'a government forewarned is a government forearmed' seriously in the digital domain, and to apply this philosophy to implicit but foreseeable ICT trends. Government often anticipates the future in its policy, and it would be to its credit to do the same, and to do so openly, in its political assessments of iGovernment.

2 WARNING FLAGS FOR iGOVERNMENT

As the process of digitization continues, it is important for government to be much more aware of certain features of information than is now the case. The point is not to focus on the information *content*, as is so often the case (with dna data requiring a higher level of protection than biometric data, for example, and biometric data requiring a higher level of protection than simple personal data such as names and addresses). Although it is important to break down information into content-related categories – as indeed happens in many of our existing laws and rules – the report focuses on information *processes*, precisely because they have a huge impact on the nature and the reliability of the information that keeps iGovernment running and on which it depends. In today's digital era, these processes have a number of features that must be taken into account when considering how to expand or set limits to iGovernment in a way that is evenly balanced.

We have therefore tagged three interrelated processes with warning flags. These warning flags are not intended to be prohibitions; rather, they are a sign that policymakers and politicians must be extra vigilant. They will help improve general 'iGovernment self-awareness': when information is either part of or the result of the tagged processes, government must pay close attention to the quality of that information and consider who bears responsibility for it. In some cases, the conclusion may even need to be that it is necessary to impose certain limits on the use of information. An evenly balanced development of iGovernment requires us to look very closely at these information processes. The three processes that we have flagged in this way are:

a The *networking* of information, i.e. the shared use and management of information within a network of actors
b The *compiling and enhancing* of information, i.e. creating new information and profiles based on different sources from different contexts
c The pursuit of a *preventive* and pro-active policy based on information, i.e. actively evaluating and intervening in society founded on an informationdriven risk calculation.

These three information processes are the core of iGovernment, enabling it to fine-tune and customise policy, obtain a comprehensive picture of the public and of the policy issues involved, and take pro-active action where needed. At the same time, they are processes that themselves have an impact on information: they influence its nature, reliability, recognisability, contextuality and traceability. Although there are no insurmountable or absolute objections to this, it is important to make sufficient allowance for the risks involved in these processes when dealing with and using that information or when allocating responsibility for it. That is very often not the case given that iGovernment lacks self-awareness. It is important to realise – much more so than at present – that it is precisely these three processes that have

a big impact on (a) the quality of information *content* and (b) the demands made on the *organisational context* of information flows. Consequently, there are a number of important conditions that can be identified for the ongoing development of iGovernment.

2.1 Quality of information content

All three information processes – the networking of information, the compiling and enhancing of information, and the pursuit of information-driven preventive and pro-active policy – require a critical assessment of both the quality and the relevance of the information produced by the systems of the various authorities. Part II discussed various tendencies and reflexes, for example: the nonchalant linking up of information files; the habitual overstepping of the boundaries between the service, care and control domains; the absence of a clear and pre-determined plan to control the unstoppable flood of information; the continuous dilution of information quality owing to repeated use; and the accumulating and mixing of many different kinds of information. In iGovernment as it has evolved in recent years, composite information circulating in networks easily crosses 'boundaries'. Those boundaries are not only territorial ones (the borders between countries), but also, and in particular, the dividing line between public and private sectors and 'their' information, and the distinction between information used for service, for care, and for control purposes. Much of this information is, moreover, decontextualised when it is retrieved from its original environment, only to be recontextualised when combined with other data in a different policy context. That naturally has consequences for the reliability and recognisability of the information. These consequences are not only felt by the professionals who work with the data (and who are obliged to interpret information taken from a different professional context), but also apply, to an even greater extent, when the information concerned is the result of technological 'reproductive processes', such as profiling and data mining. The more data and information files are contaminated – and they often are contaminated, or at least vulnerable to being so – the more networks will increase exponentially any risk associated with contaminated information due to the unique dissemination characteristics of networks. A contaminated information system will not grind to a halt on its own, after all. On the contrary, in many cases no one is even aware of the diminishing quality of the information, and it continues to be processed and reprocessed, used and re-used, again and again.

Meanwhile, both the relevant government official and the citizens in question are unaware of the deterioration. It is all too easy for the quality gap to remain unnoticed, especially in networked situations, without anyone being 'to blame'. Indeed, this may well be an unavoidable risk of what can be referred to as the 'multiplier effect' of ICT: information circulates and is effectively distributed at lightning speed, whether or not it is correct. Administrative reality and 'real reality' can diverge quite dramatically in iGovernment, and errors can be disseminated much more

quickly, making them more difficult to rectify later on. Such errors can have huge repercussions for the daily lives of individual citizens, especially if profiling is used to enhance information or pursue a pro-active policy based on faulty data.

The quality of iGovernment therefore requires constant attention and consistent policy across the breadth of government. The assumption that information is correct must be replaced, across the board, by the realisation that some information is very likely to be inaccurate, obsolete, or even misused and manipulated. The default position within government, however, is that the system always tells the truth; margins of error are ignored and citizens are increasingly held responsible for the problems that ensue. There is too little awareness of the consequences of iGovernment; the multiplier effect and the constant decontextualisation owing to the networks are not factored into the monitoring of information quality, if such monitoring takes place at all. Policymakers can also be blinded by the positive results of networks and composite information. Their concern about the quality of information should not be limited to the information itself, but should also extend to the metadata. Metadata acts as an indispensable signpost in information management systems. It plays a crucial role in tracing information and identifying the original context and origins of that information. The quality of an iGovernment information management system depends on the presence of good quality metadata. In addition, the quality of the information depends on such technical and organisational prerequisites as data security, well-designed work processes, and a reliable authentication and identification infrastructure.

Government must do more than it currently does to counteract 'techno-trust', as evidence shows that every system and every information flow has both intentional and unintentional effects, and that those effects, in turn, influence the content of the information as such. All too often, government insists – and often does so officially – that its data is correct. In other words, government trusts too much in the quality of information and lacks a healthy dose of scepticism in that regard, adding to the vulnerability of iGovernment.

Self-aware iGovernment always looks critically at its own information management systems. It regards the quality of the information and of the information processes with a healthy dose of scepticism; both must be judged continuously on their merits and improved where necessary.

The role that information plays in policy processes changes once digitization is introduced. Increasingly, information is being used to anticipate the future, a trend that is also catching on in the areas of service, care and control. In a growing number of cases, the traditional method – whereby statistics are used to inform and improve policy – is being supplemented by information-driven policy designed to predict *individual* behaviour. Information and risk calculations are used to predict which chil-

dren may be at risk and which passengers may be terrorists, for example. Action is then taken based on that risk calculation. The shift in focus to individual behaviour means that the outcome of a risk calculation may be very valuable – a life is saved or an attack thwarted – but it also means that the repercussions are extremely serious if the calculation is wrong. Anyone who is flagged in government networks and systems as a potential terrorist, criminal or abusive parent will feel the consequences in his or her daily life. There is too little awareness in government of the use of statistics and risk calculations in connection with individuals (rather than in connection with broad policy categories), and of the potential consequences of doing so.

The most dramatic examples with the most far-reaching implications are found in the area of national security and in care sectors involving life-threatening situations. But even in less precarious areas of service and care, statistical methods and the effects of networked information processing can assign individual citizens to the wrong category and retain them there for a lengthy period. These separate domains are also increasingly coming to overlap thanks to ICT, with errors being circulated and dispersed between them. It is clear as well that information is no longer as easily 'forgotten' in the everyday reality of government information management, despite the prescribed retention periods. Certain categories of personal information tend to persist in profiles and networks, with all that this implies for the individuals involved.

iGovernment must therefore keep a keen eye on the possible negative and even damaging effects of information-driven policy. Sound procedures for dealing with such policy are vital for those individuals who find themselves in a tight corner. They are also important as a way of maintaining and boosting confidence in iGovernment. They require an even balance between the principles of accountability and transparency and also require the roles and responsibilities of government and the citizen to be evenly balanced. It is important to distinguish between the role of the citizen as *citoyen* (a participant in the political life of the community) and the role of the citizen as an individual (someone who has certain legal rights and obligations). In the first instance, the citizen is a productive countervailing power who should be 'kept in the loop' as regards government policy and the role that information processes play within it. In the second instance, a citizen who is treated unfairly or improperly by government or who ends up trapped by the systems of iGovernment must be able to invoke his or her rights. Both roles require a certain amount of vigilance – a combination of watchfulness and assertiveness – to act as a counterweight to the expansion of iGovernment. Citizens cannot be assumed, however, to exercise vigilance by default; they must be supported by rights and procedures that are, in effect, the practical outcome of taking the principles of accountability and transparency seriously. Generally speaking, the citizen-*citoyen* sees transparency as a greater priority, whereas the citizen-individual gives top priority to accountability. In order to support citizens as a countervailing power, iGovernment must display a certain amount of openness about its affairs. Without transparency and access

to information, real democratic supervision is impossible. That means that iGovernment must be more open and that it must encourage citizens to think and talk more about its development, and do so at earlier stages of its 'design'. Government must do so both of its own accord and in response to vigilant citizens and organised groups that have submitted requests and followed procedures in order to gain access to information. The platitude 'you have nothing to fear if you have nothing to hide' can just as well be applied – tongue in cheek of course (after all, it is just a platitude) – to iGovernment itself. As a supervisor of government, the citizen may justifiably be expected to be vigilant and assertive; equally justified, however, is the citizen's expectation that government should be more transparent.

When a matter concerns the citizen as an individual – and in particular when that citizen is seeking justice from the state – then transparency is only the beginning. Transparency will ease the way towards being better informed, of course, but an emphasis on transparency should not mean that the wellinformed citizen is (erroneously) taken as the standard, thereby putting the onus on all citizens to get their digital affairs in order and to be unrelenting in their vigilance. The existence of a 'digital divide' alone implies that there would soon be enormous inequality between different groups of citizens. What is more, the citizen has neither the authority nor the power to change anything permanently in the networked back office of iGovernment. Experience shows that citizens are often the victims of back office errors and are powerless to correct them. It is important, therefore, to set up sound procedures relating to final responsibility for information and an unambiguous access point that enables citizens to induce iGovernment authorities to act accordingly. That involves striking the right balance between the citizen's responsibility to alert the authorities to inaccuracies (and his or her capacity to do so) and the authorities' responsibility to actually correct such inaccuracies. Particularly in the more sensitive domains of care and control (in which successes are extremely beneficial to society and errors are extremely disadvantageous to individuals), citizens should not be saddled with the unique responsibility for incorrect or obsolete government information (or its consequences). In short, government bears a heavy responsibility because it alone has the power to take binding decisions that will correct errors throughout the iGovernment network, and not only in the particular database or organisation where the problem has been detected. On the other hand, the threshold should not be too low for individual citizens either, as it will then be too easy to require officials to go to unnecessarily excessive lengths.

iGovernment must invest in procedures that will improve transparency (supporting the citizen as citoyen) and accountability (supporting the citizen as an individual with legal rights and obligations). Right now, responsibility and accountability procedures within iGovernment are inadequate and insufficiently effective; responsibility and accountability must be identified and allocated more comprehensively, explicitly, and clearly.

2.2 Embedding sustainable and fair information flows in the organisation

iGovernment self-awareness, and in particular the three warning flags of networked information, composite information, and information-driven proactive policy, naturally also have repercussions for the practical and organisational design of iGovernment. Despite the increasingly common use of the term 'information management', information flows are still not properly embedded in the organisation of government when it comes to management, quality, and the safeguards. The evolution of iGovernment has so far been 'a lot of flow, and too little management'. The flow of information throughout the organisation of government (and beyond) is growing freer, but the conditions for properly controlling and managing such flows are lagging behind. Converting paper files and filing cabinets into digitally linked information files offers new opportunities, but it also casts government's traditional duties and obligations in a different light. The work of organising and managing all the information circulating in government's databases and networks is qualitatively different to the work of managing information on paper. Information management also involves the way iGovernment's 'memory' functions, and that immediately leads to two problems. On the one hand, government is growing 'feeble-minded' and forgetting things that should not be forgotten. On the other, government increasingly 'remembers' information about citizens, the thinking being that such information may come in handy someday. The first is harmful because transparency and accountability are impossible without a good memory. The archiving function of government enables it to hand on, trace, disclose, and account for its actions. That is vitally important both internally, within government, and externally, *vis-à-vis* the citizen. In the digital era, however, archiving requires a radically different approach to government information management. The Netherlands Court of Audit has emphasised this repeatedly and offered various organisational guidelines to that effect.

At the same time, government appears to be incapable or unwilling to forget certain types of information. The inability to forget is also harmful, however, because it means that citizens may not be able to escape from their past. Government sometimes proves unable to observe its own prescribed retention periods; it is also inclined to extend these periods, based on the notion that more information equals better information. Security and fraud prevention are magic words in this respect, but there are also good reasons for government not to consider all of the past when judging citizens in the present or future. By working with profiles, government quenches its own thirst for information and makes the very act of storing and remembering information important in itself. People are much more likely to be seen as the products of their past than they were in the pre-digital era. If digital records are stored in perpetuity, 'once a thief, always a thief' takes on new meaning. The fact that it is technically possible to store personal data for ever is not a good enough reason to actually do so. Once again, we need to examine the pros and cons of storing (or deleting) information within the relevant context, and that examina-

tion may differ from one context to the next. For example, information that is used in criminal investigations may need to be scrutinised differently to information in the healthcare sector, where long-term data storage can be of enormous benefit for research and for estimating mortality risk and heredity. The next question, i.e. *how* the data should be stored (for example, whether or not it should be anonymised), is also one that should be considered and evaluated on a category-by-category basis. There is in fact not one standard for storing or forgetting all personal or other information (i.e. an *absolute right* to be forgotten); it comes down to government weighing up each situation properly and rationally and then acting in accordance with its findings.
In short, it is vital to the ongoing development of iGovernment to take its 'memory' into account. The archiving function of government must be improved, and that will require a radical turn-around in thinking. In order to decide which citizen records should be 'forgotten', government will need to constantly set off collective interests, for example security, against individual[1] interests, such as the right to be forgiven and forgotten, and to do so transparently. To guarantee that it is acting fairly, moreover, government must be more aware than it currently is of the risks associated with using obsolete data. The Dutch Government must also ensure that the organisations operating within iGovernment are continuously aware of the importance of forgetting. Organisations must weigh up the two sides (remembering versus forgetting), make their arguments explicit, and see that the results of this process are given solid organisational foundations. iGovernment must also come up with structures and low-threshold methods for helping citizens remove obsolete, incorrect and inaccurate data.

iGovernment must have a memory that is effective, sustainable, and above all fair. The importance of storage and archiving demands a radical change in culture. The importance of forgetting must be permanently acknowledged and requires a strategy that is embedded both in policy and in the organisational structure.

2.3 iGovernment's 'limits to growth'?

When iGovernment is not self-aware, its natural tendency is to continue expanding. After all, only self-awareness can induce it to set limits to its own growth. Until then, there will be no real limits to the size of data collections or on the number of links between systems; information will become contaminated; organisations and information flows will be misaligned; citizens, businesses and even government organisations will become trapped in the tangle of government data; it will be difficult to prove one's identity; and it will be virtually impossible for citizens to extricate themselves from the information that is gathered, processed, and exchanged about them. Without iGovernment self-awareness and without an awareness of what iGovernment means for the relationship between government and the citizen, there is little reason or opportunity to consider the growth of the information structure that government is building. There is also little reason to ask questions,

for example whether such growth is actually necessary, whether there is a need to set limits, and how iGovernment should continue to develop. Questions and concerns regarding the relationship between information flows and their implications will be left unaddressed even as the work of constructing iGovernment continues. But government is selling itself and the citizen short by proceeding in this manner. Moreover, both the citizen and government are left vulnerable.

The practical reality of information dissemination and linkage, and the reasonable expectation that claims will be made on data collections in the future, require government to engage in a broader assessment that (a) looks beyond any specific policy initiative that it may be considering and (b) looks beyond the current circumstances. The process of weighing up the various interests at stake in iGovernment also raises a more fundamental question: is the iGovernment that has evolved the iGovernment that we would have wanted if we had specifically planned and designed it in full awareness of the context and relationships involved? This raises another issue: are there limits to iGovernment? If so, where are those limits to be drawn, and where not? And how do we determine that?

The questions relating to limits also touch on a certain vulnerability of iGovernment that is best illustrated by the Internet. The fact that the Internet is, fundamentally, an unregulated and open network makes it virtually impossible to 'manage' it or to monitor the information circulating there. After all, anyone can access information once it has been placed on the Internet. Incorrect or undesirable information can be deleted from one's own site or perhaps (after legal proceedings) removed from someone else's, but by then it has usually already been copied and 'mirrored' elsewhere. The WikiLeaks case in late 2010 offers an excellent example of how information on a site is quickly copied elsewhere precisely because the authorities and other stakeholders wanted to restrict access to it.

The uncontrollable nature of the Internet and the fundamental consequences of such uncontrollability play a similar role with respect to iGovernment, in two different ways. First of all, they affect iGovernment itself, or more specifically, government's internal information management. That differs from the Internet in that it is a semi-restricted system and not an entirely open one. It is therefore possible to control information flows to a certain extent. However, the dynamic evolution of iGovernment today is putting pressure on that ever-so-slight controllability of information. Thanks to the networked nature of information and the merging of information flows across public-private boundaries, the semirestricted system of iGovernment is growing increasingly similar *internally* to the Internet. A growing amount of information belongs to everyone in the system rather than to only a single organisation, making the job of properly guiding information flows virtually as difficult within iGovernment as within the Internet model.

As this trend continues, it will become more difficult for government to channel, verify and guarantee the reliability of information. Alongside the risk of iGovernment 'internalising' the logic of the Internet, there is another risk: that iGovernment will unintentionally become *part* of the Internet. The WikiLeaks affair once more provides a striking example, foreshadowing what will undoubtedly happen more often in future. Thanks to WikiLeaks, the authorities' internal information management system suddenly became public property on the Internet. Copied countless times and migrating rapidly from server to server and from cloud to cloud, information circulated beyond control. Dutch versions of WikiLeaks have already turned up that leak government documents anonymously and confidentially, for example *www.opennu.nl* (www.opennow.nl). Only methods such as those applied by the Chinese government might succeed in putting the genie back in the bottle, and even that is uncertain – to say nothing of whether it would be desirable. Before government information is actually leaked on the Internet, the risk of disclosure is thought to be a question of data security and the technology and policy required to effectuate it. Once sensitive information is leaked and disseminated on the Internet, however, policy is pushed aside and the authorities start to improvise in order to regain control. It is a rather unedifying sight. The pressure that the US government put on service providers to remove WikiLeaks from the Web led Amy Davidson of *The New Yorker* to ask whether "Lieberman feels that he, or any Senator, can call in the company running *The New Yorker's* printing presses when we are preparing a story that includes leaked classified material, and tell it to stop us. The circumstances are different, but not so different as to be really reassuring."[2] Nevertheless, digitization has made such leaks virtually unavoidable, and they will, unavoidably, become more frequent in the future: the 250,000 pages in the possession of WikiLeaks would have never been leaked in the same manner or on the same scale if they had existed only on paper. It is digital compression that makes information mobile and permits major leaks of this kind. Many earlier notorious cases of leaked information, for example in the UK, also concerned huge volumes of personal data stored on a lost USB stick no bigger than a cigarette lighter. The fact that leaks are unavoidable – whether they are intentional or due to error, carelessness or gross negligence – and, in particular, the consequences of such leaks are reason enough to consider the limits to iGovernment.

Although we will not identify those limits in the report (that is a matter for politics), we can indicate the general areas that should be considered. Our purpose, in other words, is to raise awareness and to spark off a debate about such limits, and not to identify precisely where they are. After all, what was most valuable about the Club of Rome's report *Limits to Growth* was that it put the environmental problem on the political agenda, and not that it made precise predictions and extrapolations. The processes identified in previous chapters offer us some preliminary guideposts for identifying where the limits might lie: we are, in effect, being forced to think about the limits to iGovernment when we weigh up the various principles involved

and observe the warning flags indicated. Although it has now grown common (albeit largely unnoticed) to mix service, care and control and to cross the boundaries between the public and private domains, these tendencies too turn out to be problematical when examined more closely and from the perspective of iGovernment. Finally, the realisation that the Internet has created a completely different information environment in which iGovernment too must function gives us every reason to analyse the nature of iGovernment and to act accordingly. Well-reasoned limits are extremely important here, not least because they give the authorities something to go on when identifying the right way to deal with information or to share it with other parties (even those in government). Right now, that is often left open to interpretation. For example, the Tax and Customs Administration decided not to exchange information within a partnership of various parties assembled by a local authority with a view to clearing a travellers' camp.[3] Tax and Customs did not feel it had the right to share sensitive information with an electricity company or other private parties; as a large, autonomous government department, it defined its own 'absolute' limits and pulled out of the negotiations. Another example is the Dutch Supreme Court's ruling (described in Chapter 7 of the report) on the Public Prosecutions Service's requisitioning of passenger data from Trans Link Systems.[4] It should not, however, be left to bottom-up campaigns or isolated judicial rulings to set such limits or to define the framework for the ongoing development of iGovernment. After all, if Tax and Customs or Trans Link Systems had agreed to provide the information as requested, the data exchange would have quietly taken place, without any further discussion.

A self-aware iGovernment cannot exist without there being a well-reasoned strategy regarding the limits to that same iGovernment. Such limits are required by both the internal dynamic of iGovernment and the dynamic of the iSociety: without limits, government will ultimately lose the ability to guide the ongoing development of iGovernment in manageable channels.

2.4 An agenda for the transition to a self-aware iGovernment

It is urgent that 'iGovernment self-awareness' become ingrained governmentwide, both as a concept and as an organisational factor. The danger, however, is that such awareness will be cancelled out by the political issues of the day. Given what is at stake, that would be an unfortunate turn of events. In order to act on the recommendations given above, government must transform its existing system of public administration into one capable of identifying and tackling the challenges that iGovernment brings. The organisational and administrative effort involved will require the engagement of many different organisations and levels of government. In other words, our recommendations are not intended solely for the Dutch Government. The national authorities can, however, *drive* the search for solutions. In addition, iGovernment is now so dynamic that it must have sufficient leeway to rapidly integrate new developments and the responses to such developments into

its thinking. 'iGovernment self-awareness' is not just a status to enjoy, but rather an ongoing challenge. In a world of rapid and dynamic digitization, however, it is important to create various champions that (a) claim stewardship of 'iGovernment self-awareness' and (b) provide iGovernment with a well-defined, authoritative point of contact and recognisable identity.

The institutional landscape as it now exists is not equipped to create such champions. At its core, iGovernment consists of interrelated information flows and networks – and it is precisely on that point that we lack organisations that are willing and able to concern themselves with the integrated whole. The political debate is broken down into laws, areas of policy, Parliamentary committees, and technologies; only rarely does it consider the overall information picture, let alone any existing or future links between information flows and their consequences. The same compartmentalisation applies with respect to the funding for digitization projects, and consequently for how funding is managed and influenced. There is no 'Ministry of Information' or 'Parliamentary Committee on Information'. Ministries, government agencies and other local and regional authorities are primarily concerned with their own policy problems and spare little thought for the consequences of incoming and outgoing information flows that reach beyond the 'limits' of their own duties and organisation. The same can be seen in cross-border contexts. The European network of information flows and personal data is expanding and diversifying without there being any frank discussion as to whether, how, and under what circumstances the Netherlands will participate in the emerging iEurope. Government agencies use the information they obtain in communication with citizens, but they are powerless to trace errors in information flows and correct them throughout the entire chain or network when the same citizens run into problems. The many different supervisory bodies (for example the Data Protection Authority and the Office of the National Ombudsman) and other organisations such as the Identity Fraud Helpdesk, which identify and attempt to resolve some of the excrescences of iGovernment on behalf of citizens and government agencies, are often simply not equipped for the task in that their responsibilities do not reach far enough, and are in fact incapable of producing solutions (or at least lasting ones). Crossministry programmes and other arrangements, such as the Reinforcement of Public Sector Identity Chain policy programme (*Versterking Identiteitsketen Publieke Sector*, VIPS), are only temporary, and in many instances are not sufficiently high-profile in terms of bureaucratic stature. Not one of them has the authority to implement its methods or solutions permanently across the boundaries of ministries and institutions. Government also lacks the expertise needed at the policy-technology interface to develop new systems that are 'iGovernment-proof'. Brave attempts are made at all these levels to consider iGovernment in its entirety, to conduct proper assessments, and to search for solutions to problems, but the existing organisations and arrangements are unable to meet the challenges of iGovernment because they have not been assigned the necessary statutory duties or the authority to take binding decisions. There is therefore an urgent need to develop an agenda for institutional

transformation. Government must catch up with practical reality by transforming itself institutionally from eGovernment into iGovernment. It needs institutions that will allow it to channel the discussion on the ongoing development of iGovernment in the right direction, to claim responsibility for its own networked information management system, and to provide citizens with a form of protection that takes the properties of iGovernment into account.

Fleshing out the targets for iGovernment will therefore require an institutional transformation that assigns and embeds three functions within government:

a the *strategic function*, i.e. guaranteeing the well-considered, ongoing development of iGovernment;
b the *societal function*, i.e. making iGovernment more transparent for the public and improving its accountability vis-à-vis individuals who become entangled in information networks;
c the *operational function*, i.e. improving well-reasoned connections between policy, implementation, technology, information flows, and networks. Also, improving the commissioning practices of government.

These three functions constitute the absolute minimum requirements for shaping iGovernment self-awareness and acting on the implications of the new reality. The following section offers specific proposals for these three functions, along with the necessary institutional 'mechanisms'. It should be noted that the institutional transformation as such – which involves embedding aims and facilitating implementation – is ultimately more important than merely the labels for the organisations proposed here.

iGovernment requires the system of public administration to be transformed, with existing arrangements being redesigned at the strategic, societal and operational levels.

3 iGovernment institutions

iGovernment as it has evolved in recent years certainly does not lack for institutions. Our analysis in Part II of the report involved a procession of government organisations and did not even mention an equally large number of organisations that are concerned in various other ways with ICT and government. All these institutions and organisations do their work as best they can in their own specific area. The problem is that – like iGovernment itself, which has evolved largely without a pre-determined design or plan – many of them have also emerged spontaneously along with iGovernment or have been added piecemeal. In the same way that iGovernment has developed application by application and link by link, so too has the institutional landscape evolved in response to individual applications and the related opportunities and problems. These organisations are in fact eGovernment – and not iGovernment – institutions. However: they do not have the same relation-

ships and links that are such important features of iGovernment. That is true both for the way they have developed and for the way they exercise supervision and enforcement. Although many organisations are dedicated to promoting the opportunities of ICT or to highlighting the disadvantages and risks involved, as a group they are not sufficiently effective. The individual organisations scarcely acknowledge that their own work is related to the work of the others, let alone explicitly refer to that relationship in their mission or in the action they take.

One important conclusion that we can draw from our arguments above is that the networked nature of iGovernment makes it extremely difficult to control from a central point. Hierarchies and networks are uneasy bedfellows. At the same time, something or someone must drive iGovernment self-awareness forward, the implication being that this should be a national body with the authority to take binding decisions. The challenge, therefore, is to identify institutions that can combine the logic of networks and the power to take decisions, within both government and the broader social context of iGovernment. iGovernment operates against the backdrop of an iSociety that is influenced by and in turn influences ICT. In addition, government's public information networks often flow over into the private networks of businesses and citizens. iGovernment cannot be structured autonomously and in isolation. All the relevant actors must be involved – not only those within government but also stakeholders in the private sector and the citizen. The motto must therefore be: 'Make sure we involve the iSociety in building an iGovernment to last'.

If we follow the report's line of argument to its logical conclusion, then the only real institutional recommendation that we can make is that iGovernment selfawareness must seep down into every government organisation and into every vital point in the process of digitization, from the initial plans drawn up at the national or international level or the first sketches for a new application to the specific assignment or contract and, later on, to the linking up of information. iGovernment self-awareness must be ingrained throughout: that is the aim. Such awareness grows by means of an evolutionary process that can be accelerated by external factors, for example (as we have seen in other countries) the uproar surrounding the publication of confidential government documents by WikiLeaks, or a major scandal relating to information management. But the growth of that awareness can also be encouraged by establishing institutions specifically designed to act as drivers.

In this final section, we describe the general outlines of four institutions capable of driving iGovernment self-awareness. The strategic, societal and operational functions are allocated to four new organisations that must be given the power to shape the transformation of iGovernment. As indicated above, recognising the urgency involved and developing an associated agenda are more important than hammering out every detail. The biggest priority is to allocate the strategic, societal and opera-

tional functions to institutions and to equip these institutions with the necessary means and the power to take binding decisions. It is against this background that we make four proposals for iGovernment institutional innovation: to allocate the strategic function to a permanent committee for iGovernment that reports to the Senate and House of Representatives; to allocate the societal function to a national iPlatform and an iAuthority, the first being responsible for transparency and the second for dealing with and resolving problems that citizens encounter with iGovernment; and finally, to allocate the operational function to an organisation responsible for ensuring professional commissioning practices in government.

3.1 Permanent committee for iGovernment

The responsibility for promoting iGovernment self-awareness must be allocated to a national organisation. That is because, in any scenario, there is too great a risk that such awareness will be dissipated among the particular interests of the various actors and organisations that concern themselves with ICT and its consequences.

Set up a permanent committee for iGovernment that reports annually to Parliament on 'the state of information'.

The main task of such a committee would be to note trends and developments, recognise how they are related, and think them through from the perspective of iGovernment, i.e. beyond the boundaries of ministries and levels of government, and with a view to potential future developments. The committee's advice would focus specifically on the 'warning flags' described above, i.e. networked information, composite information, and preventive and pro-active policy. Its annual report would be made available in the public domain and offer information-related (as opposed to technology-related) recommendations relating to government's plans, viewed within the broader context of iGovernment and iSociety. Where relevant, its advice would specifically consider European and international trends and developments. Decisions taken at these levels often only emerge as topics of political and social debate in the Netherlands at a much later stage. Because they influence how iGovernment and its branches beyond the Dutch borders develop, however, they should be noted, discussed and thought through at a more appropriate point in time.

The committee's agenda must involve more than just advising on planned measures, however. One recurring item would be to evaluate ICT projects – whether up and running, abandoned, or completed – in the light of information flows and the relationship between service, care and control. The very fact that iGovernment consists of ongoing processes of linking and diversification makes it crucial to keep close track of projects and links, draw lessons from the past, and encourage the relevant debate. Ideally, that debate should concern function creep and similar matters, with function creep being recognised both as an inherent feature of innovation and

as a problem – i.e. opposite sides of a coin that can be confusingly similar at times. Drawing on the annual reports of the iPlatform and iAuthority (see further on), the committee would also take stock of situations and systems in which citizens (and companies) have run into difficulties and, at a more general level, draw lessons from such cases and monitor them for improvement or deterioration. One specific point to watch for would be the all-too-common tendency to evaluate ICT projects strictly from the narrow perspective of the technology or the budget involved. The committee must focus much more explicitly on facilitating and carrying out evaluations that consider whether the new application in fact delivers the information specified by the underlying policy objective. If the aim is to embed 'iGovernment self-awareness' throughout government, then a willingness to learn is more important – at least for the time being – than any accountability mechanisms.
The committee's report would be discussed in both chambers of Parliament and in the presence of the committee's chairperson. It would be up to the House of Representatives to draw conclusions from the recommendations. The Coordinating CIO would run the committee's secretariat, as this would create an institutional relationship between iGovernment self-awareness in the Government and in Parliament. The new task would also boost the strategic position of the Coordinating CIO and improve his or her forward-looking capacity.

The Office of the Coordinating cio could help establish a broad public forum to support and assist the committee. The forum, an advisory body, would nurture the relationship between the permanent committee for iGovernment and the iSociety. Following the example of the broadly-based Standardisation Forum – set up to support the Standardisation Board – the iGovernment forum would provide the permanent committee with ideas, express its concerns, and suggest solutions. The forum would be made up of a wide range of stakeholders and experts. In addition to representatives of ministries, government agencies and local authorities, it would also include experts from the private sector (not representing specific businesses but based on the particular expertise that they can bring to the table), scientists, supervisory bodies, and 'citizens', i.e. NGOS such as the Consumers' Association and human rights organisations. In 2001, the Docters van Leeuwen Committee suggested setting up a similar body (which it called the 'Platform for the Electronic Society') to advise a government commissioner (ICT and Government Ad Hoc Advisory Committee 2001). At the time, the Government rejected this proposal, pointing out that the Minister for Urban Policy and Integration played a coordinating role with respect to ict. In its official comments, the Government concluded that the Minister would provide a more effective institutional anchor. But that argument no longer holds water. iGovernment represents a break with government's tradition of thinking in terms of eGovernment; the approach it requires differs from the role that a coordinating minister can or may even want to play. The networks that make up iGovernment, whether internal or external, and recognition of their impact make for an agenda that should not be restricted to a single ministry or

even exclusively to government. iGovernment will become a matter of coordination only when self-awareness of iGovernment has been well and truly embedded throughout the system.

3.2 iPlatform and iAuthority

There is strong evidence that an enormous 'back office' of government information flows has been created, which sometimes extends beyond the boundaries of government. As mentioned above, much of the information in these networks has been 'abandoned', in the sense that no one claims responsibility for it. It is sometimes impossible for citizens to correct erroneous information, even though they are confronted with the consequences of such errors in their dealings with government. In addition to the extreme cases of identity fraud that make the headlines, there are numerous other situations in which citizens have attempted to correct contaminated government information but did not know where to turn. The organisations that should be there to assist these citizens are limited in scope and ill-equipped for their task: some are only temporary; others do not deal with individual cases; many of them operate with barebones staff and funding; and none of them is empowered to take binding decisions that will actually correct errors in the underlying network. Even the Office of the National Ombudsman, after reviewing the most publicised case of identity fraud (the Kowsoleaa case), had to admit the impossibility of correcting erroneous information once and for all.

But the 'abandonment' issue goes beyond erroneous information alone. It also applies to the information that government communicates to citizens through a patchwork of websites, e-helpdesks and Web portals. A growing number of these projects involve multiple parties (including private-sector actors) and have arisen without the benefit of democratic legitimacy or decision-making. In many of these new networked communication models, and in the communication that takes place through them, there is no clear allocation of official responsibility for the information made available. The societal function can be implemented by properly organising transparency and accountability in a way that protects citizens against falling victim to those elements of iGovernment that they can neither fathom nor influence.

iGovernment transparency and accountability must have an identifiable 'home'. Citizens should have access to a single platform that concerns itself with transparency and a single authority that is responsible for accountability.

In the same way that government is attempting to provide its service through a single helpdesk, it should also consider concentrating responsibility for transparency and data correction in a single access point or portal. That would mean clustering government forums that are currently dispersed over different websites and that tend to be application or problem-driven[5] at a single digital location. The iGovern-

ment Platform would serve as an interactive source of information about the use of ICT in the relationship between government and the citizen. To increase transparency it would clarify to citizens what kinds of records are held on them in the linked systems of iGovernment, who has access to those records, and why – and provide that information through a clear and unambiguous information portal. Following the example of the Tax and Customs Administration's allowances portal, such a Platform would allow citizens to alter and correct their personal data themselves within a secure environment, and it would also guarantee that those alterations will then be implemented throughout the entire network. Making the transparency function interactive would also empower citizens. Adding interactivity to the platform would reflect a broader tendency in iSociety, with digitization improving and driving the potential for citizen empowerment.

The second societal function, accountability, is active and has already been advocated by the National Ombudsman (2009). The iAuthority must ensure that any misrepresentation of citizens in the back office or other systems is actually corrected. Citizens must literally be relieved of the burden of rectifying and solving problems that creep into the chains and networks of iGovernment. This proposal represents a radical centralisation of accountability. The existing procedures and methods – whereby errors that have crept into the network must be corrected locally and via different institutions and supervisory bodies – have proved to be inadequate. The new iAuthority must combine expertise and a personal approach with the power to take binding decisions *vis-à-vis* the organisations that populate the back-office network of iGovernment. It is very important that the iAuthority should in fact possess such authority; if it does not, it will be given the same run-around as the hapless citizen, and the problem would simply be shifted on to another's shoulders rather than resolved. Careful thought must also be given to the degree of access that the citizen should have to the iAuthority. On the one hand, it should be a recognisable and low-threshold institution; on the other, too low a threshold makes it all too easy for certain individuals to throw a spanner into the works of iGovernment,[6] given the amount of effort that the model requires on the part of the administrators.

The iPlatform could act as a digital extension of the current government portal *mijnoverheid.nl* (mygovernment.nl). In organisational terms, the iAuthority should be set up as an autonomous body with the power to take binding decisions. All existing information platforms and operational organisations (including the Identity Fraud Helpdesk), should be merged into or combined within these organisations. The iPlatform and the iAuthority would publish a combined annual report describing their work and the results they had attained and reviewing the most important trends and developments of the past year.

3.3 Professionalising commissioning practices

Ultimately, iGovernment self-awareness must also be extended to the technical

realm, i.e. with respect to the development of standards, applications, and links between data and information flows. This is the operational function. It is, after all, the engineers and systems designers and the relevant national and international bodies that determine what iGovernment will look like at the operational level. The realisation that the relevant decisions are essentially political or policydriven is often cancelled out by the notion that technology is nothing more than an instrument. Anyone who follows the flow of information – as we have done in the report – knows that technology gives rise to categories and that 'categories have politics.' That means that questions of design, standardisation and interoperability are all decisive for the way iGovernment develops as a whole, and not just for individual applications and decisions. One of the critical elements in the evolution of iGovernment is the quality of government commissioning practices in the field of ICT. By specifying the requirements for a new system or application and identifying what functions it must have, government is in fact setting the stage for future applications and how they fit into the broader context of iGovernment. Government faces a dilemma in that respect: on the one hand, it wants to be in charge of development, for example via the ICTU; on the other, it is impossible and impractical for government itself to have all the necessary technical knowledge in house. Most of the technical specialists who 'work for government' are in fact external consultants and experts. The result is over-investment in technical knowhow and too little concern for the interaction between policy, implementation, and technology in information flows.

Government's commissioning practices must therefore be remodelled: instead of investing in technical expertise, it should invest in knowledge at the interface of policy, implementation, and technology. If it aims to take systematic action to solve ICT problems, then it will have to turn its attention from technical development to professional outsourcing. That means that the technical side of things must be left largely in the hands of parties that operate outside government (by contracting these external parties to develop applications or by purchasing applications in the commercial marketplace). Instead, government should learn how to frame an assignment; accurately define the specifications, legal context and underlying conditions; place the assignment in a broader context; and provide professional supervision during development. It is up to the developer to ensure that the technology actually works, but it the commissioning party's job to ensure (by supervising and guiding the work) that the technology generates the 'right' information and facilitates information processes that fit in well with the relevant policy and with the wishes of the agencies or other organisations that will actually implement it. This means setting up an organisation that is responsible for government commissioning practices and that is not limited by the boundaries between ministries and individual agencies. Such an organisation would employ a small group of 'core' ICT specialists and legal experts in ICT matters who understand iGovernment. That core group would be joined, on a project-by-project basis, by the CIO and other of-

ficials from the relevant ministry, and by the agency staff who will ultimately have to work with the system. It would seem obvious that the partners in the chain or network should always be involved in developing a new system or application, but in fact this rarely ever happens. Here too, the information flows generally outstrip the relevant organisations.

iGovernment must improve its commissioning practices by investing in knowledge at the interface of policy, implementation, and technology, rather than by investing purely in in-house technical expertise and development capacity.

4 IMPLEMENTING iGOVERNMENT

If the Dutch Government is to take on board the reality of iGovernment and become capable of prudently guiding its development, it must make the transition from eGovernment to iGovernment in thought, word and deed. For government to tread the path of digitization with confidence, iGovernment self-awareness will need to be embedded at every level. Government faces a crucial challenge in that respect: it must be willing and able to move the focus of debate from technology and individual applications to a new level, i.e. to interrelated information processes and linked information. What is essential is to create enough leeway and generate enough interest in weighing up the driving, underpinning and processbased principles and to do so with an open mind. Scrupulous development of iGovernment cannot proceed without such an assessment, and it is vitally important to consider iGovernment as a whole. In addition, government must exercise particular caution, both in this assessment and in its policymaking and policy implementation, whenever the three processes of information handling noted in the report come into play. These processes – furnished with symbolic warning flags – are associated with a) the networking of information, b) the compiling and enhancing of information, and c) the pursuit of preventive policy based on information. The specific implications that these processes have for policy implementation, the position of the citizen, the quality of government information management, and the internal and external reference points for liability and accountability make it vital to look critically at the usefulness, necessity, and impact on society of digitization projects.

To support government as it meets this challenge and ensure the necessary institutional grounding, the report lays out an agenda for institutional transformation. The institutions proposed within the context of this transition are intended to guarantee that iGovernment is equipped with the tools it needs to foster selfawareness, protection, and innovation. It must be clear that the institutional transformation as such is much more important than the specific form and nametags of the institutions proposed in this volume. The transition will need to take place at three different levels: the strategic level (by installing a permanent committee for iGovernment), the societal level (via an iPlatform responsible for transparency and an

iAuthority responsible for accountability), and the operational level (by instilling professional commissioning practices in government and prioritising knowledge at the interface of technology and policy above technical know-how). Finally, in the case of both the challenge that government faces and the necessary institutional transformation, the development of iGovernment cannot be viewed as separate from the path that the iSociety as a whole is treading.

NOTES

1 That is ultimately also a collective interest, because a society that does not forgive and forget is a fundamentally different society to one in which people are permitted to start again.
2 In a statement, Senator Joseph Lieberman said that providers such as Amazon (which had hosted WikiLeaks) should cut all ties with WikiLeaks. "I will be asking Amazon about the extent of its relationship with WikiLeaks and what it and other web service providers will do in the future to ensure that their services are not used to distribute stolen, classified information"; see "Banishing WikiLeaks" by Amy Davidson in *The New Yorker*, www.newyorker.com/online/blogs/closeread /2010/12/banishing-wikileaks. html#ixzz174 smobqa, requested on 10 December 2010.
3 Interview with Peter Wijntje and Sjoerd Peereboom (Ministry of Finance/Tax and Customs Administration), 19 October 2010.
4 LJN: bk6331, Dutch Supreme Court, 08/04524 B.
5 Examples include *burgerservicenummer.nl* (for the BSN), *infobsnzorg.nl* (for the EPD), *lastvandeoverheid.nl*, *mijnoverheid.nl*, and the Identity Fraud Helpdesk for the public.
6 Cf. discussions on (among other things) environmental organisations and their sometimes disruptive access to the administrative courts.

III AFTERWORD: iGOVERNMENT AND iSOCIETY

In essence, this publication is about government taking responsibility for the way it uses ICT. The role that government plays in the information society and the responsibility that it bears go much further, however. In addition to being accountable for iGovernment, government is also responsible, to a certain extent, for the way the iSociety as a whole functions. Such sweeping responsibility can be defined in terms of the following questions: What aspects of the information society should government be concerned about? Should it intervene? If so, how? Former Dutch Prime Minister Wim Kok addressed this issue in April 2001 at the Infodrome Conference: "We must nevertheless ask ourselves what responsibilities government will face in the years ahead in connection with the consequences inherent to the information society." That responsibility can be described as the system responsibility that iGovernment has for the iSociety. Any intervention in the iSociety will naturally be politically charged and to a certain extent controversial, but an attempt must nevertheless be made to find common ground for matters that government is obliged to guarantee. iGovernment's system responsibility cannot simply be ignored.

That is because, first of all, government must stand up for its citizens when the private sector fails to adequately guarantee their interests. For example, the growing power over information exercised by such global corporations as Google, Facebook and Apple will force government (and the European Union) to consider whether – and if so how – that power should be restricted in the public interest. There have already been certain moves in that direction. Responding to questions raised by Parliament in August 2010, the then Minister of Economic Affairs Maria van der Hoeven undertook to ask the Data Protection Authority (CBP) to evaluate a new clause in Apple's privacy policy.[1] In some cases, questions touching on government's system responsibility will need to be addressed at the European level and through a European actor (a 'lead authority'[2]) because it is only the European Union that has the necessary weight and authority to take forceful action. However, the popularity of interactive communication in social networks and through Web 2.0 raises another question: is it government's responsibility to control or restrict the behaviour of citizens and/or to protect them against commercial actors in that sphere? To a certain extent, moreover, government's system responsibility in these and other cases can be legally enforced as a human rights matter (De Hert 2011).

"It is not true that European jurisprudence offers the authorities too little in the way of specific guidelines. The Court of Justice has formulated general principles concerning the protection of personal data that are being applied in a growing number of cases. The same is true, to a somewhat lesser extent, of the battle against identity fraud and the protection of media pluralism. The Netherlands can make good use of these principles" (De Hert 2011).

How iGovernment should interpret its system responsibility is in our view, the key issue – we've moved beyond the question as to whether it should do so at all.

Secondly, system responsibility becomes an issue when trends in the private sector interfere too blatantly with crucial government policy. Cases in point are the various advances in the area of identity management. Government is making a major investment in digital identity tools, for example the biometric passport, the DigiD system, and (potentially) the eLicence. It is precisely because it is investing heavily in identity authentication – and makes claims as to its accuracy – that government must also concern itself with identity authentication in the semi-public and commercial sectors, in particular where there is a risk that the quality will deteriorate. What is the point of investing in the data security of a national database under the terms of the Passport Act, when the same data is also generally available beyond the domain of government? The introduction of the biometric passport raises questions about the use of biometrics in the private sector. Little has been done to regulate such use, and politicians have so far ignored this issue. Swimming pools, supermarkets, employers and computer manufacturers, for example, will be at liberty to experiment with new applications.

The growing stockpile of information also makes identification an increasingly important key for linking and combining data outside the context of government. Experience shows that the use of digital identities is blurring the boundaries between the public and private sectors. The impact of that use is therefore spilling over the same boundaries, especially when private-sector actors have duties under public law (civil-law notaries) or when government requires private actors to establish the identity of individuals – under the Compulsory Identification Act (*Wet identificatieplicht*; provision of services; employment) – based on the identity documents issued by government. For example, the BSN was conceived as an identity authentication code for government services; no one considered the possibility that it would very quickly catch on as a universal (public-private) unique identifier. For these and other reasons, government must keep a careful eye on trends outside its own territory and consider whether and when stricter guidelines or rules are required. "It is not true that European jurisprudence offers the authorities too little in the way of specific guidelines. The Court of Justice has formulated general principles concerning the protection of personal data that are being applied in a growing number of cases. The same is true, to a somewhat lesser extent, of the battle against identity fraud and the protection of media pluralism. The Netherlands can make good use of these principles" (De Hert 2011).

The fact that government bears final responsibility in such cases does not mean that it must take matters solely into its own hands (De Hert 2011) or even that it has the capacity or leeway in its own organisation to do so (Meijer 2011). There are, however, a number of pitfalls that it must try to avoid with regard to this fundamental

responsibility. First of all, ministers must think hard before deciding to intervene. Government naturally has a duty to intercede in societal relationships (in this case informational relationships): that is one of its *raisons d'être*. At the same time, however, such intervention can be risky: it can be thwarted by social dynamics for all kinds of reasons, and government must anticipate such a possibility. Secondly, it would be risky to adopt an 'ICT user's mentality' at the start of an intervention. The information society – the ICT-immersion of everyday life – does not 'belong' to government in the way that its own ICT systems do, and government must be aware that there are constitutional aspects that need to be taken into account when it decides to intervene. Thirdly, there are different ways to intervene, and it is all too easy to choose the wrong one. To start with the most traditional scenario: government can decide to intervene in informational relations by imposing mandatory regulations. It can also take a 'soft' approach, however, and merely offer itself as an interlocutor for private players. The middle ground between the two extremes is facilitatory: it can create the right basic conditions for society to work out its own potential solutions. Each of these *modi operandi* is based on a different conception of responsibility.

According to Meijer (2011), however, it is becoming more difficult, and indeed perhaps impossible, for government – as the actor bearing system responsibility – to play a key role in the turbulence and complexity of technological networks. "Instead of overall responsibility, government can increasingly claim two other responsibilities: procedural responsibility and miscellaneous responsibility." Procedural responsibility means that government would no longer be responsible for outcomes, but merely for the quality of the process. Miscellaneous responsibility would allow government to guarantee that those involved are making an effort to protect citizens and prevent system failures. It would involve government taking on the duties that others have failed to fulfil. The permanent committee for iGovernment proposed above could play an important role in setting the agenda for the concept of government system responsibility. The key questions that the committee would address are: what trends and developments in the broader iSociety should be encouraged or discouraged, and what is the most suitable level for taking regulatory action (national or international)? Which general trends and developments can be expected to trickle down to iGovernment and what does that imply for any regulatory action?

However, certain iSociety trends will increasingly force government to face fundamental questions that it has not even begun to answer. The speed at which information is disseminated and copied – even (or especially) when it is unwelcome to government – means that the authorities will also have to consider their own information management system. The WikiLeaks affair has made that patently clear. Transparency is generally regarded as something that government concedes to citizens (passive transparency); it is not often considered a virtue worth practising

(active transparency), and certainly not something that only a handful of citizens can claim or force from government. In today's digital world, however, the authorities will increasingly have to consider precisely how they intend to deal with transparency. As John Naughton commented in *The Guardian*, the authorities must "[l]ive with the WikiLeakable world or shut down the net. It's [their] choice" (Naughton 2010b). They are not likely to choose the latter option. Nevertheless, they will need to find a new balance between freedom of the press, data confidentiality and data security; a regulatory system may be an option. Part of the answer may lie in regulating parties outside government (servers, clouds etc.), but part of it may also require government to engage in self-examination. Some information should perhaps not be stored at all; other information sources should be more transparent rather than confidential and secret; and still other information should be stored more securely than it currently is.[3] But government can never entirely rule out the unpredictability and uncertainty of society and, consequently, the iSociety.

When it comes to iGovernment's responsibility for the iSociety, the frame of reference is the same as when assessing government's use of ICT. In essence, we can define government's system responsibility by – once again – weighing up the driving, underpinning and process-based principles, although in this case the driving principles often operate beyond the boundaries of government. The public and businesses move ahead, inspired by the promise of new technologies and profits. When this drive is not offset against underpinning principles or kept in check by the process-based principles that make information flows transparent for the public and – if necessary, open to criticism – then those responsible for iGovernment should at the very least ask themselves whether the time has not come to take action.

NOTES

1 Memorandum by the Minister of Economic Affairs responding to questions about a new clause in Apple's privacy conditions, 3 August 2010.

2 There are now arguments within the EU in favour of a "lead authority" with sufficient powers to resolve these sorts of issues for the 27 Member States (interview with J. Hennis-Plasschaert, Liberal Party (VVD). Formerly MEP, now MP in the Dutch House of Representatives, 4 November 2010).

3 As suggested by Bits of Freedom (among others) in its analysis of the WikiLeaks 'Cablegate affair'. See Ot van Daalen, *De wereld na Wikileaks' Cablegate*, at www.bof.nl/2010/12/10/de-wereld-na-wikileaks-cablegate.

IV ORDER iGOVERNMENT

iGovernment (ISBN 978 90 8964 394 0) is available in bookstores and from Amsterdam University Press, www.aup.nl/info@aup.nl. The full version of the publication is downloadable on www.wrr.nl.

Amsterdam University Press

How does the use of ICT affect the relationship between government and its citizens? The report *iGovernment* analyses the developments of networking information and concludes that in everyday practice an iGovernment has gradually come into existence, overtaking the old paradigm of the eGoverment. The iGoverment, effectively running at full speed on information flows and networks, is however seriously out of step with the self-image of the digital government, and the existing structure and division of responsibilities.

This synthesis is based on the report on iGovernment that the Scientific Council for Government Policy (WRR) presented to the Dutch Government in March 2011.

"This book contributes powerfully to the understanding and evaluation of the development – beyond 'eGovernment' – of 'information Government', centred on highly complex flows and uses of information for public services, care and control, rather than technology itself. Sound empirical research and a concern to create better governance of iGovernment enable the authors to bring a sharply critical eye to their call for greater awareness by policy-makers, and for a strategic, reasoned and institutionalised relationship among the principles involved. These include ones that are often neglected: privacy, freedom of choice, accountability and transparency. Their recommendations are important, not only for the Netherlands".

Charles D. Raab, Professor Emeritus and Honorary Professorial Fellow, University of Edinburgh

"This book will be a valuable resource for researchers and scholars seeking to understand the possibilities, dilemmas and challenges of bringing the Internet and related technologies to centre stage in government and public services. It offers a fascinating case study of electronic government and 'information government' in the Netherlands, with examples from local, national and EU government, a wide-ranging literature review and a number of recommendations as to how iGovernment should develop".

Helen Margetts, Professor of Society and the Internet and director of the Oxford Internet Institute, University of Oxford

"Not only does this book offer an insightful analysis of the problems that ongoing digitization poses for citizens and the government itself (such as creeping loss of data quality), it also places highly valuable markers for the decisions that must be taken on the challenging path that lies ahead for iGovernment, in providing a new model for weighing up the various fundamental interests at stake".

Alex Brenninkmeijer, National Ombudsman, The Netherlands

WRR

SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY

Lange Vijverberg 4-5, PO Box 20004, 2500 EA Den Haag
telephone +31 (0)70 356 46 00, fax: +31 (0)70 356 46 85, e-mail: info@wrr.nl, website: www.wrr.nl