Editorial

Public Administration in the Information Society: Essays on Risk and Trust

Miriam Lips, John A. Taylor and Frank Bannister

1. Risk, trust and the state of public administration

Risk and trust are interlocking issues, thrown into the social, political and managerial foreground as governments pursue their responses to the development of the information society. Transformations in the ways in which information is gathered, stored, transmitted and shared throughout government and the wider polity raise a variety of concerns across the spectrum of scholarship and public commentary. As the use of ICT becomes virtually ubiquitous, debates about risk and trust have taken on deeper and broader dimensions, in part reflected in the growing interest in risk management, and more recently in trust management, in public administration.

Risk and trust must be acknowledged as central concepts in governments' ambitions to address the information society, therefore. As our societies, polities and economies become increasingly 'wired' and information intensive, the collection, management and development of information resources come more and more to the centre of attempts to control and regulate for risk and trust in and by public administrations. Flows of information deriving from new ICT applications pervade public administration and the wider polity, as the chapters in this book show. Indeed we are reaching a point where practising public administrators see remedies for major arterial blockages in the governmental body increasingly to be found in new forms of digital networking, of which the Internet perhaps provides the greatest opportunities. As these potential remedies are identified and implemented so it becomes ever clearer that governmental risk management is at the heart of many of them. Moreover, and as a concomitant of its management of risk, government is also seeking to manage trust, in particular the trust levels of citizens and consumers, not only of its own services, but those of the commercial world. As governments better manage risk so, it is assumed, the trust of citizens in those governments will rise.

Risks are omnipresent, both within the government machinery itself and externally to it. Government has a responsibility to deal with both. These risks can be macro in scale, such as the risk of losing public confidence in government, and micro, such as the risk of failure of a new government computer system. This macro/micro scale is a scarcely adequate bifurcation, however, for macro risks can have a myriad of micro consequences and vice versa. Moreover, management of these risks often can be reciprocally related to the management of trust, for to manage risk will contribute to increased trust and to manage trust implies the reduction of risk. Combining risk and trust management, opens up new management perspectives on emergent issues in the information society.

In the practice of public administration, risk and trust are pervasive and their management crucial. High quality information is critical to that management. To know more about these issues, to communicate more effectively about them and to implement far-reaching public policy measures, all require the further intensification of information management from which this enhanced risk and trust management can be realised. Yet, such information intensity in its turn introduces new risks. As the depth and breath of information passing through systems in public administration increases, new risks emerge and old risks can be amplified. Amongst these risks is loss of public trust. The management of risk and trust are crucial to effective public administration.

This volume explores a range of risk and trust issues emerging from contemporary developments in the management of information, information flows and resources in public administration. It does so in the form of a series of essays for which scholars were invited to explore widely, independently, uninhibitedly and even provocatively, the profound questions faced by both practice and discipline in public administration. As is clear from these essays, the challenges for governments are formidable, as is the search for effective solutions. These challenges must be confronted, however, if we are to have effective public administration within a society simultaneously labelled risk society and information society.

2. A collection of essays

By intention and design this volume of essays draws together perspectives on ICT developments with risk and trust management in contemporary public administration, perspectives that have either been largely ignored within the discipline or, equally inexplicably and unsatisfactorily, kept separate.

The origins of the book are to be found in plans laid in 2003 for the annual Study Group on ICT and Public Administration, held under the aegis of the European Group of Public Administration [EGPA] conference. For that meeting we encouraged scholars to try and fuse established perspectives on ‘informatization’ in public administration with emergent perspectives on the implications for public administration of societal, political, governmental and managerial risks and related issues of trust. The better the understanding that public administrators develop of the organisational, political and democratic impacts of e-government service delivery and the experience that consumers have of those services, the greater the chance of success of such systems and services. Equally if politicians, administrators and service professionals are to develop new ways of controlling external risks then better intelligence and information are essential. For governments to assess and manage the risks that arise as a result of informatisation requires that they have high levels of understanding of both internal and external operating environments and the relationships between them.

Clear perspectives informing both the conceptualisation and design of academic research and public policy formation, are crucial to influential research and effective public policymaking. Currently, however, in the discipline of public administration, major ambiguities, uncertainties and lacunae prevail in the key perspectives that concern us in this volume. From both the informatisation perspective, which must include the role of the Internet in modern government, and risk and trust-related perspectives, there is little agreed scholarly or practitioner understanding, leaving the discipline in a state of theoretical and conceptual incoherence and thereby limiting opportunities for useful, policy-informing research and improved policy implementation

This collection of essays is a first joint attempt of scholars in the broader field of ICTs and public administration to address these shortcomings. It is our hope that these essays will help both to develop our thinking and provide new insights which will in turn shine new light on the challenging, highly complex questions public administrations are facing in the developing information society.

3. Structure and contents

The contributions in this book fall into four sections, each of which we examine at greater length below. In the first of these our contributors examine issues of risk and trust. They do so by looking both at how government must understand the issues of risk and trust that it faces and also at how government finds ways of managing risk in its search for higher levels of trust. The second section looks at how information is being managed in new ways in different policy domains of government so as to mitigate risk, on the one hand, though introducing threats to personal privacy, on the other. The third section captures a further aspect of practice in contemporary public administration, that of the search for innovation. Information is a source of innovation, for government as well as for other sectors but, as government innovates in ways designed to reduce risks of failure, so new risks emerge – as these chapters show. The essays in the final section address overarching issues relating to Internet governance. How is the Internet governed, and how adequate is that governance? Is the formal governance of the Internet suborned by the *de facto* governance of what are fast becoming the world's largest companies – the computing and media industry giants whose own technical standards may be acquiring the status of universal industry standards, with far-reaching consequences both for the industry itself and for individual and collective forms of government?

3.1. Risk and trust

Issues of trust, including the lack of popular trust in government, have always been an important consideration in shaping the structures and practices of governance. It is therefore not surprising that the impact of information and communication technology (ICT) applications on public trust – what Dutton et al. in this volume refer to as 'cyber trust' – is a crucial element in the take-up and effectiveness of e-government services. The continuing debate about identity cards in the UK provides an example of widespread, identifiable public concern about the degree to which government can be trusted with the stewardship of information, including personal data, about its citizens.

At the heart of these concerns about trust in e-government is a 'trust tension' caused by the simultaneous need to collect data on individual citizens as the basis for providing public services, such as health and taxation records, and fears of data surveillance, including the inappropriate secondary use of personal information held in these records. Thus, according to these authors, governments must engage in 'trust enhancing strategies' that include the provision of 'learning opportunities' in cyber- service consumption for citizens and the establishment of clear guidelines for public service organisations that will reassure citizens, thus enhancing rather than undermining trust.

The gaining of citizen trust by government may, however, be more a matter of political rationality than logical prescription. In their contribution to this volume Taylor and Burt take us to what they call the 'trust diamond', a two axis, four point diagram. On one axis we see the relationship between government, at one point, and non-governmental agencies producing and providing electronic services on behalf of government, at an opposite point. On the second axis lie trust and blame. The authors argue that government may simultaneously reduce the negative consequences of assigned blame deriving from service mistakes and failures whilst raising up their trust level amongst citizens by off-loading high risk service delivery to non-governmental providers. This strategy for simultaneous blame avoidance and trust enhancement is most likely to succeed where such non-governmental providers are from the highly trusted voluntary sector. Here we have risk management through 'government by association'. Enlisting respected and trusted bodies from the charitable and voluntary sectors associates trust-starved government with highly trusted organisations, with the additional advantage that if mistakes and failures do occur within these transferred service arrangements, the blame does not fall directly upon government.

This essential social and political relationship between risk and trust is explored further by Bekkers & Thaens. Following Castells' analysis of the network society they argue that the mutual dependencies by which the information society is characterised are seemingly sustained by the existence and development of forms of social capital and the reciprocal trust relationships that derive there-from. Yet this perspective holds major problems within itself, as a further characteristic of the network society is the breaking down of the social identities from which social capital derives. Thus the socio-economic benefits that derive from the enhanced flexibilities and fluidities of the network society are set in counterpoint to the atomising tendencies of such a society with its consequent reduction of socially value- adding reciprocities and trust relationships. In this interconnected world of the network society, government must contend with risk that is both broadened and deepened, with events occurring that 'spin' and 'snowball' around these networks, including internationally, and thereby beyond the control of any single node [or government] on the network. Powerfully and persuasively, these authors argue that the governance of risk in this complex interconnected world has to be pluriform in nature. Differentiated, though interconnected, networks and infrastructures are cut across by differentiated policy regimes, themselves characterised by varied governance strategies. Models of risk management must take into account this mosaic. Prescriptions based upon a single focal point are highly vulnerable to failure.

3.2. Risks to privacy in new forms of information management

How can government secure its citizens and make them safer and at the same time shore up their rights to enjoying a private domain? This is a crucial question in an era in which government has to recognise the need for new forms of information management that seem to have diametrically conflicting goals. Enhanced informationabout service consumers, particularly consumers vulnerable to forms of criminal or anti-social or personal threat, provides government with new high order moral opportunities: as information is gathered, managed and used in new ways governments can choose to intervene in ways that protect citizens. Yet to know more about the citizen, in particular to focus holistically upon the citizen through the medium of information, is also to run into dilemmas about what government needs to know about the individual citizen. Is there a point in the gathering of information about citizens beyond which governments should not go if they are to avoid unnecessary intrusion into that citizen's personal sphere?

The two chapters in this section cover these and other related questions. Bellamy et al. address how government agencies pursue their goals through the development of enhanced information resources gathered through new forms and intensities of information sharing. So-called 'multi-agency' initiatives have been formalised across a host of social policy arenas, initiatives whose 'glue' is information exchange and sharing. The authors refer to the increased surveillance capacity of government that this information sharing represents, though they are hesitant about the extent to which one might argue that such sharing reduces personal privacy. The key to this plethora of initiatives is a form of risk management that the authors refer to as *"precautionary intervention"*. To step into a particular private situation before a public offense or misdemeanour arises is laudable, working as it does with the grain of the age-old question of how to deliver the theoretical efficacies attaching to joined up government. However, can such precautions lead to an undesirable increase in 'false positive' identifications with the numerous unfortunate possibilities that might accompany them? The risks here therefore are to be found in the possibility that more and more individual citizens will find themselves under a public spotlight that may prove unjustified or unwarranted. Risks are also evident in the loss of professional judgment implied by these shifts. As professional work becomes increasingly 'information driven' does the essence of professionalism, the ability and willingness to offer expert judgment, become reduced?

Bannister's contribution to this volume comes to the dilemmas raised over informational privacy in the context of the search for enhanced security in a more full-on way. Risk and privacy are to be found on the opposite scales of the balance. To raise up and seek to resolve issues of enlargement in the perception of social risk may well result in the relative lowering in importance of the protection of personal privacy. To raise up issues relating to the primacy of personal privacy may well result in the lowering in importance of risk assessment and risk management. A society that places primary importance on personal privacy can be expected to be one that is more risky whilst one that attaches larger significance to the management and reduction of risk may well be one in which the citizen is more constrained – more 'watched', more 'intercepted', more 'dossiered' or 'read about', as Bannister says, and more the subject of the softer side on information monitoring, that of intelligence with its strong requirement for the interpretation of personal data.

Looking through the lens of risk assessment Bannister offers up *"a number of mechanisms for achieving a better balance between the right to individual privacy and the need for communal security in an information society"*. Governments should introduce a 'privacy council', made up of societal stakeholders, whose specific function would be to manage on society's behalf the balancing between risk related encroachment into the personal sphere, on the one hand, and the 'palisading' or enlargement of the personal domain, on the other. Such a council would be sensitive to the core substantive point, but would be so whilst recognising its role in specific historical, socio-economic and political contexts. Secondly, Bannister calls for legislation and regulation that has potentially injurious consequences for personal privacy to be time limited in its force, thus requiring regular re-thinking of the imperatives under which such legislation is established. He links this point too to a third proposal, that of the need for improved forms of monitoring of government practices that impose themselves upon personal privacy. Fourthly and finally Bannister proposes more and better research and social debate on these matters so that they might be better informed. The essence of the call therefore is that personal privacy as with any 'currency' can be traded, but that trade is sufficiently significant from a societal perspective that it must be proportional. As in any regulatory regime therefore the principle of proportionality must be invoked repeatedly in a period in time and between such periods. To lose a sense of proportion in balancing risk and privacy is to risk the loss of deep social value and for citizens to find themselves subsequently unable to restore such value, able only to lament its passing.

3.3. Information, innovation and risk

We stated earlier in this opening chapter that *prima facie* information is a resource whose possession and management enables the mitigation of risk. Information is the balm applied to the risk society, a transcendent ameliorative that can in one application reduce the riskinesses of the modern polity. We now look again at this proposition through lenses provided by our contributors to this volume within this third section and conclude that the proposition does not indeed hold up under scrutiny. Searching for new ways of using information, as well as for new ways of enabling it to be communicated, often brings its own risks, whether through failures in the vast investments made in the development of new information systems, through overly simplistic appreciation of what is made possible by new flows of information in the democratic arena or through too little attention being paid to the unintended consequences of innovative information systems.

In her contribution Margetts revisits issues relating to the uptake by government agencies of new information systems and the dismal performances of so many agencies in their commissioning and subsequent adoption of new systems. These failures sit as a backdrop raising up a plethora of performance risks as well as risks that follow from public perceptions of 'failing government'. Margetts identifies three main ways in which many of these risks might be grouped. First are the risks that follow from government lagging behind in what Margetts calls the 'smart society' – failing to keep up with the business sector and an increasingly sophisticated and demanding citizenship thereby failing also to adopt the business imperative of 'knowing your customer' and being inflexible in the face of growing demands for more shaped and customised services. Secondly she discusses the failure to understand the complexities of new system building with 'third party' partners, failures that introduce new risk elements including those attaching to the nature of the partnerships involved. Thirdly, she examines the failure to recognise the embeddedness of information technology and systems in public policy to the point where policy and systems failures (and successes) are utterly interwoven. All of these failures, and indeed the risk of failure so inherent in new large-scale systems developments, can only be mitigated by new strategic understandings. New modes of contracting, new approaches to government learning and strong forms of within-government leadership are required.

In his contribution, Coleman takes us to an area that historically, in academic writing at least, was a progenitor for discussions of IT in the polity – that of 'electronic voting', now though, mostly thought of in terms of 'on-line' voting. The field remains, as it always has been, divided into the zealots, the believers in the power of technology to record and sort the citizen vote accurately and efficiently, and the sceptics pointing to the array of risks and pitfalls which always accompany technological solutions to the long standing problem of how to engage the *demos* in democratic societies. Coleman takes us away from this confrontation into an array of questions that are central to any evaluation of the risks of such developments as voting on-line. Let us be clear, he argues, about who is at risk, about the sort of democratic outcomes that are at risk. Let us ask whether the risks are purely technological or whether there are other matters at stake. We also need to ask 'in which spatial sphere is the risk greatest?' For the bulk of his essay Coleman takes us through these questions helping us to analyse and clarify the issues raised by on-line voting. Indeed he takes us further by asking what risks attend inaction, i.e. what are the risks in remaining with traditional methods of recording the vote? The rich tapestry woven by Coleman in this volume helps both to sort out the multitude and differentiated nature of perceived risks attaching to on-line voting and to open the debate about this aspect of modern democratic expression., a debate which he believes needs to be more widespread.

Meijer's essay examines, in very grounded ways, how the Internet can help mitigate risks in the everyday life of the citizen. His concerns are less about offering prescriptions for improvement or in sorting out the nature of high level democratic debate. Rather his paper asks an immediate question about whether in the specific case of offering neighbourhood detail in the form of a map to be found by citizens on the Internet, what might be termed 'social transparency' can be enhanced, thereby leading on to assuaging risk for the individual and the family in the neighbourhood? Meijer is especially interested in government responses to this new form of transparency and whether new forms of risk management by government accompany these maps as a consequence of real or presumed pressure from individual citizens and citizen groups. In his own country of The Netherlands, as in many other countries, local factories have suddenly and entirely unexpectedly been the cause of local tragedy. So how does new risk mapping, and the transparency that accompanies it through Internet access, affect these locally hazardous activities? Skilfully in seeking an answer to this question, Meijer invokes the rule of 'anticipated accountability' and shows how both governments and private companies react to this new form of transparency despite little demonstrable public or citizen concern being expressed. Here, he argues, public transparency and accountability are enhanced because of these reactions and the risk management measures taken. Thus the citizen is safer. A paradox exists within this reaction, however, as increased safety may coincidentally lead to lower security as, for example, terrorist groups also use this mapping data to identify potential targets. Thus the risks related to safety of the citizen, the family and the neighbourhood may reduce whilst the security risks to those same agents rise.

3.4. Risks to Internet governance

The final section in this volume takes on a series of macro issues relating both to *de jure* and *de facto* ways in which the governance of the Internet takes place, issues that are, at the time of writing this particular chapter, being debated publicly, not least in respect of the influence of a single country, the US, in the regulation of this vastly important global network.

Lips and Koops trace the short history of Internet, from early public utterances that seemed to interpret it as a phenomenon amenable to unique regulation in single countries, to the current recognition of its global ascendancy and the need for regulatory bodies and instruments to be similarly placed on a global footing. Their concern is to locate the debate about Internet governance within a clear understanding of the democratic and legal risks that this medium introduces. To do so they concentrate in their essay on the layers of Internet governance made manifest in a plethora of organisations and suggest that *"not only is [the well known] ICANN's situation unclear regarding the transparency of authority and related decision making powers. Other Internet organisations also have organisational structures and arrangements which make it difficult to grasp where responsibility and accountability lie".* The authors conclude that the current modes of Internet governance are unsatisfactory, placing as they do so much power over Internet architecture and rules in the hands of scarcely understood bodies with at best fuzzy forms of public accountability.

Prins and Schellekens focus upon crucial, legally-derived issues of Internet governance in their essay. As they explain, the Internet consumer is often at the end of a long chain of Internet actors with each of these actors in some [weak or strong] sense responsible for content. At each link in the chain however is the potential for legal challenge as links such as Internet Service Providers (ISPs) or Payment Systems seek to 'regulate' Internet content or process. The authors cite a recent case involving PayPal – *"On September 13, 2004, Internet Law News reported that the US financial intermediary PayPal was going to levy a 'fine' of up to $500 on customers who violate its use policies – i.e. on those customers who use PayPal to pay for gaming, pornography* (*'adult content'*) *and pharmaceuticals from unregistered pharmacies [2]".* This initiative they argue is *"a clear sign of the growing pressure on Internet intermediaries to introduce enforcement policies against bad and/or untrustworthy Internet content. And this in turn raises the interesting question of what exactly 'bad' or 'untrustworthy' Internet content is.*" The establishment and verification of high levels of trust, enforced under law, is therefore crucial to the effective operation of the Internet. But how is this best achieved given the legal risks that inhabit so many of the links in the Internet chain? The authors point to the insufficiency of the liability approach to the proffering of unreliable information on the Internet. Rather, they argue, a new approach must be found, one based firmly in the principle of self-regulation. Criteria for establishing the reliability of information on the Internet must be established and enforced, though this is much easier to write than to enforce. As they write, [we have shown] *"... that the step from reliability criteria to enforceable norms that regulate the behavior of the providers of information appears far from trivial. The very characteristic of information is that it is so flexible and diverse that it seems to resist every attempt to* *regulate it.*" Here, then, is yet another layer of risk in the governance of the Internet. As new codes and regulatory instruments are developed and supported by parliaments so the core of the problem, the nature of information itself, may indeed prove beyond robustly enforceable regulation.

Finally in this volume we have the essay from Hoff and Bjerke which raises major concerns, including new risks, relating to their development of the concept of 'media citizenship'. In an era where political life in all its forms is intensely mediated for the citizen by many media outlets and in which the facility for expression, involvement and engagement can be made more possible through these multiple media channels, a new form of citizenship, media citizenship, seems applicable. As the authors state *"[media citizenship] should function as a democratic norm alongside and in addition to the form of citizenship we normally associate with the fundamental rights in Western welfare democracies, i.e. civil, political and social rights"*. But, do the de facto governance structures of the Internet severely inhibit and distort such citizenship? That is the question to which Hoff and Bjerke devote their essay.

At the core of the concerns about Internet governance and the realization of a strong media citizenship is the suffusion into everyday life of computer programmes through which information is stored, structured and presented. Control of both software development and its deployment become crucial therefore to the ways in which information comes to be handled and comprehended. Social discourse in its myriad forms can be highly structured by this deep communications infrastructure, therefore, with 'ways of seeing and doing' in large part pre-determined by it. They argue that copyright protection is currently one way in which such pre-determinations occur. Major companies in the media industry are now trying to create software platforms designed to protect commercial interests that simultaneously and necessarily exclude other market entrants and thereby other consumer choices. Following the well-known work of Lessig, they argue that legal code and software code are becoming synonymous, thus enshrining and realizing the commercial interests of some over others and unintentionally restricting other forms of creativity from which the citizen might otherwise benefit. Thus the mitigation by large media industry companies of commercial risks relating both to copyright and competition results in their replacement by profound social and political risks. Implied in the developments that they write about is high level control over the citizen when using the Internet. In 'western democracies' the Internet is becoming more and more the access point for news, entertainment, information, political discourse, and many commercial products and its regulation, particularly perhaps more hidden or *de facto* aspects of that regulation becomes of crucial social significance. As the world's largest media companies shape the Internet through new software solutions to 'problems' of copyright and competition, and as legislatures create rules and laws that sustain the interests of these giants of the information age, so the idea of media citizenship within the idealised forms that many have expected and wanted is not only put at risk, but perhaps lost forever.

4. Conclusions

Of course, conclusions to this volume are to be derived by readers. We asked our scholars to write in the form of essays so as both to provoke the reader's interest and to be highly accessible in explaining the positions that the authors take. We believe that authors have succeeded in meeting these goals. These essays should provoke us into thinking more deeply about the risks inherent in an information society, at so many levels of that society, and to realise how closely related to the management of trust these matters are. Their scope encompasses the management and governance of risk and trust: from risks affecting a single country to those that are global; from risks to the individual citizen, to those to society as a whole; from risks that can be narrowly defined and responded to, to those that relate in complex ways to other conceptual domains that have major importance in democratic societies, such as trust.

What we might describe as an information society could also be called a risk society, as the essays here show. By fusing these two perspectives in eleven scholarly essays we hope to have contributed both to a vital debate and to advanced scholarly and popular understanding.