Foreword

TRUST, TRANSPARENCY AND COLLABORATION:
THE ETHICAL CHALLENGE TO THE INFORMATION SOCIETY


2007 may come to be seen as a pivotal year for e-government. The pivot was that curse of politicians- unexpected and destabilizing events – anticipated by some experts, but unheeded in many ICT programme developments. It was the year that the drive for e-government services suffered a series of highly media-sensitive setbacks, despite the surge in people using the Internet for both public and private purposes, especially retail uses. In the public domain there is the UK Government, for example, scoring well in international benchmarking, and moving to consolidate its own dispersed websites into two, one for citizen services, the other for business services. But despite such advances, a series of data losses on a large scale, with some data turning up in the USA, raises questions about how citizens and their children can be fully protected in what has been an open, often outsourced data management culture. These problems are having a political effect also, with large-scale IT schemes, such as the national identity card project, and the on-going IT for Health project in the NHS, coming under closer scrutiny from all sides. Even in the private sector, the problems of on-line fraud, e-banking security concerns as exemplified by the Societe Generale affair, and identity theft risk denting the wider need for trust among customers. A realisation is emerging that citizens’ needs and customers’ demands are not quite the same thing. Questions are being asked about control, accountability, trust and security, not just at national and international level but within regions as well. These will assume an even greater urgency and political potency when the sharing of data across borders by public administrations is accelerated in the years ahead. People will demand even greater control over cross-border data management systems where their personal data is concerned. This has profound implications for political cultures within countries and within collaborative inter-state constructs such as the EU, demanding a new culture based on citizen-centric expectations understood, acted upon and protected by their e-government guardians.

REBUILDING THE BRIDGE OF TRUST

If 2007 was a pivotal year for data assurance management, 2008 and beyond will be years when a range of questions will be raised entwining technology and politics as never before, and with civic concepts such as trust, security, fairness and transparency bridging both technology and politics.

The following list of questions will inform the debate:
• How secure is the whole outsourcing process, when personal data is handled in India, the USA, or wherever?
• Should lower costs determine the outsourcing process?
• Should ‘efficiency gains’ continue to take priority over the needs for security and access?
• Under what rules and conditions are data held and exchanged in the countries and companies which handle data on EU citizens, and people from around the world visiting the UK?
• How accountable are companies, including non-EU companies working for EU governments, to the taxpayer and governments when major security leaks occur?
• How adequate and sufficient are financial penalties or criminal penalties to encourage robust baked in security from the outset? How fast can they be updated to keep pace with technological advances?
• How do parliaments scrutinize major e-government programmes? Is scrutiny enough to ensure real accountability or is accountability no longer possible?
• How can legitimate concerns among citizens be addressed?
• How can vulnerabilities in remote and online transactions be addressed to decrease fraud and the exponential rise in cybercrime?
• If current e-government projects are judged to be insecure within a national context, what chance is there of getting popular support for either exchanging data at the EU level or for automated European interoperability between public sector data systems?
• How can the socially excluded and disadvantaged, the disabled and an aging population be expected to keep in step with and collaborate with e-government procedures, if they fail to provide the essential requirement of trust and reliability in handling individuals’ data?
• How does government restore confidence in its ability to manage large IT schemes, and create alliances with citizens on benefits of both cost and service?
• What can we learn from other countries, especially other EU member states and regions?
• What lessons might be learned from studying the CNIL in France, a national watchdog on the impact of Internet-based technologies on citizens’ privacy?
• How will states cope with Article 8 of the Services Directive, which will implement Internet-based service provision cross-border?
• Should citizens be able one day to monitor and even control some key aspects of their data held by government?
• What are the objections to allowing citizens to be in control of access to and the release of their personal data?

NATIONAL AWARENESS ENHANCED BY EUROPEAN ENGAGEMENT

Just as research informs innovation and development in the private sector, so its effect in government needs to be understood and selectively utilized, where it brings benefit. But too often policymakers fail to appreciate the relevance and applicability of many research projects and recommendations. Instead, they seem to prefer the recommendations of private-sector consultants and miss, through lack of awareness or a tendency to seek the traditional private ‘solution,’ the evidence of research funded by government itself in universities and national research laboratories, or research funded by the EC often with key inputs from the UK’s research community.

There has never been a better time to engage in a process of mutual learning. Most major government projects now involve large ICT commitments and components. The European Data Protection Supervi-
sor regularly identifies and reports on privacy and data handling weakness and solutions. Governments and citizens are anxious about and perplexed by ICT-led developments in biometric identification in passports and other ID domains, data management, fraud and ID theft, never mind the future challenge of the Internet of Things at the very time when there has been a massive increase in international mobility. Rather than being surprised by events in the future, it is essential that, within the EU, governments are alert to, engage with and shape, not just the ICT, but also the citizen-centric implications of the implementation of Article 20 of the EU Treaty on diplomatic and consular protection for citizens, moves towards a Common Consular Space and an EU External Action Programme, cross-border healthcare provision, judicial and police collaboration, and convergent standards for EU passports and visas. The internal borders of the EU have been largely dismantled; now the electronic barriers need to be removed. But just as recent referenda indicate that EU citizens have often felt left behind or just ignored in the rush to implement the single market and the euro programme for business, so this next challenge must involve the security, well-being and trust of the citizen as a prerequisite not just of administrative success but of the e-governed’s assent to extend their civic rights into regulatable cyberspace.

**BETTER NATIONAL PROTECTION AND PERFORMANCE INFORMED BY EU PROGRAMMES AND PROJECTS**

A number of initiatives funded by the EC demonstrate the capacity to test, criticise and question the ways governments tackle national challenges, by taking a wider, Europe-wide view informed by good practice from public-private consortia, experience and piloting. Often such projects involve the evidence of small countries with pioneering experience of e-government. Below are some EC national and regional projects from which other states and their regions can benefit in shaping their own domestic e-government programmes:

- The Burgerkarte and successful e-government projects of Austria
- The e-justice EC project (2004-6), and e-justice programme piloted again by Austria
- Secure e-voting in Estonia
- The FIDIS project and its implications for biometric identification
- The SecurEgov project into security for pan-European interoperability systems
- The Challenge project examining implications for e-governance on traditional democratic institutions and procedures
- The eGovernet project led by Sweden into e-government research in the EU
- The recently launched STORK project into e-ID
- The R4eGov Integrated Project into secure e-government data exchange interoperability at scale between member states and agencies
- The Hadrian project in the North East Region of England, a private-public partnership approach to restoring trust in ICT-led business and bureaucracy

**CONTROLLING TECHNOLOGY, RENEWING DEMOCRACY**

This book addresses how we can meet some of the challenges mentioned above by using technology to create and sustain alliances within trust-based collaborative structures. Understanding the tools available, and how we can better harness them for such tasks means that much of this volume addresses the techni-
cal sphere. For this, no apologies, because it is only with better instruments, those which already exist and also those we need to invent, that we can advance the trusted agenda of the e-governed. The Internet has created wealth, mobilities, and opportunities for work, leisure and learning at an unparalleled scale. It has also spawned a rash of global threats and intrusions into our everyday lives, creating apprehension and insecurity. Research which can help decision-makers and governments to learn, constantly, how best to build collaborative trust between themselves and their citizens or clients is one important pillar in rebuilding trust in the Internet age. And it is not just trust in the process of data management which is at stake, but trust in the clear and stated ability and resolve of democracies to master for its peoples their entitlement to the widened, secure, and better life offered by the Information Age.

Andrew Robinson
European Consular and Commercial Office, UK
Member of the EC Integrated Project R4eGov (2006-9)
into eGovernment secure interoperability systems

Andrew Robinson is Hon Consul for France in the UK, and adviser on European and international strategic opportunities to both private and public sectors. His wide experience with EC programmes extends over 20 years experience, including most recently major EC research projects such as eJustice and R4eGov, both of which inform his Preface to this book. He is Chairman of the European Consular and Commercial Office, and joint creator of the first Franco-German Consulate in the EU in 2004. He is also a Member of the Fraud Forum in NE England, introducing the importance of cross-border interoperability, trust and security, which informs much of his current professional work. He is a Chevalier (Knight) of the Order of Merit, and the Chevalier of the Academic Palms by the French Government for his services to Franco-British and European collaboration. His career spans senior posts in universities, government service, and the private sector.