Chapter 13
Citizen Centric or Government Centric?
Perceptions of Risk in New Identity Management Systems

Ruth Halperin
London School of Economics, UK

James Backhouse
London School of Economics, UK

ABSTRACT

This chapter explores citizens’ perceptions of information risks inherent in the move towards eGovernment that deploy identity management systems (IdMS). The new plans for electronic identity management in the UK sparked a furious public debate but the related perceptions of citizens have not yet been systematically explored. The findings presented in this chapter were developed using grounded theory methods of open-coding content analysis and depict how a sizeable group of UK citizens regard the risks. Five areas of perceived risk emerged and they testify to the diversity of issues and concerns preoccupying citizens: technology failure, public authority competence, public authority integrity, lack of control over personal data, and, the overpowering state. Further, the authors present findings that express how citizens might ultimately act in the light of their perceptions. Drawing on social risk theory and current political developments, the authors discuss these emerging perceptions and suggest that citizen-centricity and joined-up systems - central to the transformational government agenda - stand in considerable jeopardy and require the government’s attention and a suitable response.

INTRODUCTION

As the move towards eGovernment gathers pace in UK and other countries around the world, the impact of the digitalisation of many citizen-state interactions is beginning to challenge accepted wisdom on what digital citizenship consists of, what its risks are, and how they might be managed in the new digital era. The aim of this chapter is to explore the information risks perceived by citizens, identity risks in particular, that are seen to emerge from eGovernment vision and its underlying systems. We define information risk here as the harm
that may arise from the loss of confidentiality, integrity or availability of information under public custodianship.

An important characteristic of eGovernment applications is its dependence on technologies for managing identity. eGovernment, and its current UK variant, tGovernment (transformational government) is predicated on the collection, storage and use of personal information on citizens. For tGovernment to succeed, ‘means must be provided for citizens and businesses to engage electronically with government via secure networks that maximize user confidence and respect data protection requirements. A system of authentication of electronic documents must also be planned and developed’ (Saxby, 2006:1). Hence, tGovernment projects must deploy electronic identity management systems (IdMS) in some form or another.

Major plans for digital identity management were tabled by the UK government as part of the Identity Cards Act, 2006, including a new central database – a National Identity Register (NIR). Personal information identifying every UK citizen is to be stored on the NIR, which will allow data sharing between governmental agencies and authorized organizations (Crossman, 2007). Data sharing, which underpins the joined-up government concept (Six et. al., 2005), is one of three themes in the UK tGovernment strategy (Transformational Government, 2006). Citizen-centricity is another such theme, and the two are closely linked:

We must be relentlessly customer-focused. Many people want a single point of contact for a range of services. The public are not interested in whether their needs are met by department X or agency Y, they just want a good, joined-up service where X and Y talk to each other and share the information the public have provided. We should strive to meet this demand’. 

Sir Gus O’Donnell, Cabinet Secretary (Transformational Government, 2006: 14)

The notion of citizen-centricity or customer-focused services, central to the eGovernment agenda, is epitomised in systems such as CRM (consumer relationship management) (Bose, 2002) extensively adopted from the private sector into the UK public sector (Lips, 2007). CRM relies on identity technologies, profiling systems in particular, and their claimed benefits mirror many of the objectives of the new tGovernment programme (King and Cotterill, 2007: 339). Likewise, the national identity card is supposed to achieve a broad set of benefits for the individual citizen: ‘protect your identity from theft; protect vulnerable people from those who have lied to gain positions of trust; speed up many everyday transactions; make it easier for you to travel in Europe; make the internet easier to use; make it easier to replace lost and stolen documents’.2

However, despite the citizen-centric rhetoric and the proposed benefits, the implementation of new IdMS also brings with it new risks. We argue that understanding how the risks arising from new IdMS deployed in eGovernment are perceived and addressed may be critical to citizen acceptance of eGovernment. Large-scale systems have proved to be failures when end-users practise resistance during implementation (Bauer, 1997). A UK research programme, “Ensuring privacy and consent in identity management infrastructures”3, currently under way, lent support to this view that without consent, acceptance will be difficult to obtain. An identity system for the UK should be based on public trust and user demand rather than on enforcement of criminal and civil penalties. The winning of public trust could be realized, in part, through the creation of a more flexible citizen-centred model45. Therefore, citizen perceptions, their fears and expectations, have important implications for any future attempts at implementing eGovernment systems deploying IdMS, as they may well result in resistance to use, misuse, or non-use.