Managing Citizen Identity Information in E-Government Service Relationships in the UK

A. Miriam B. Lips a; John A. Taylor b; Joe Organ a

a Victoria University of Wellington, School of Information Management & School of Government, Wellington, New Zealand
b Caledonian Business School, Glasgow, UK

To cite this Article Lips, A. Miriam B., Taylor, John A. and Organ, Joe'Managing Citizen Identity Information in E-Government Service Relationships in the UK', Public Management Review, 11: 6, 833 — 856
To link to this Article: DOI: 10.1080/14719030903318988
URL: http://dx.doi.org/10.1080/14719030903318988
Abstract

Governments are introducing new digital Identity Management (IDM) systems into public service relationships with citizens. These IDM systems not only can support governments in their modernization efforts, they are also expected to lead to significant informational changes in the citizen–government relationships. Thus far however, there is little empirical knowledge available about what changes are occurring in these emerging e-government service relationships as a result of using new IDM systems. With that, important questions arise as to how ‘citizen identity information’ and ‘identity management’ are being reconstructed conceptually in new forms of public service provision; and what the managerial, governance and democratic implications are of the deployment of these digital IDM systems in the relationship between the individual and the State. This contribution provides some empirically supported answers to these important questions.

Key words
Citizen, citizen identity information, e-government, identity management, public service
INTRODUCTION

Governments throughout the world are introducing new digitized identification and authentication systems into e-government and other public service relationships with citizens (e.g. Birch 2007; Halperin and Backhouse 2008). Well-known examples are smart cards, biometrics, web-based e-authentication systems and CCTV cameras. These new Identity Management (IDM) systems are being managed and used to supplement, and sometimes to override the need to display, traditional forms of personal identification and authentication, such as a passport, driver’s licence and birth certificate. To governments, the technological capabilities of these digital IDM systems offer opportunities to represent, collect, store and use citizens’ identity information in new ways and forms (Taylor et al. 2006, 2007; Lips 2008).

With the introduction of these new IDM systems governments not only perceive opportunities to enable the modernization of their organization, they also see advantages of transforming their service provision to the citizen (Varney 2006). A well thought out approach to IDM is expected to bring a wide range of possible benefits to government agencies, including improved efficiency and effectiveness in public service provision; innovation and joined-up service provision; enhanced information security and privacy; improved customer convenience and access to public services; and, last but not least, a step increase in the provision of e-government services by enhancing trust and confidence in online interactions with citizens (OECD 2009).

The introduction of new digital IDM systems may not only bring about benefits to government agencies however; they are also expected to lead to significant changes in the relationship between the citizen and the State (LSE 2005; House of Lords 2009). The potential benefits referred to above can have a substantial impact on legal rights and other citizenship-related entitlements: on privacy, anonymity, security, public safety or even on citizens’ trust in government, to take some examples (e.g. Bennett and Raab 2003; Lyon 2003b; 6 et al. 2005; Backhouse and Halperin 2007; Clarke 2009; Cofta 2009). Consequently, advances in technological capability embodied in these new IDM systems, coupled with increased public safety and security threats, may bring about substantial informational imbalances in citizen–government relationships to the disadvantage of the citizen (LSE 2005; Crossman 2007).

Thus far however, there is little empirical knowledge available about what changes are occurring in these emerging e-government service relationships as a result of the application and use of new IDM systems. With that, important questions arise as to how ‘citizen identity information’ and ‘identity management’ are being reconstructed conceptually in different e-government service relationships; and what the managerial, governance and democratic implications are of the deployment of these new digital IDM systems in public service provision to the citizen.

This contribution aims to provide some empirically supported answers to these important questions. In section two, an overview will be provided of traditional forms of identity information on the citizen and the management of this information in public
service relationships. We then will explore emerging forms of citizen identity information together with contemporary understanding of the informational changes that may occur in e-government service environments as a result of the introduction of new IDM systems. Third, we will look at seemingly opposing scholarly perspectives on the implications of the introduction and use of new digital IDM systems in citizen–government relationships. Based on the same contemporary understanding of informational trends in emerging e-government service relationships and their fundamental change implications, scholars, supported by UK practitioners, have developed different viewpoints on the direction and outcomes of the application of these informational trends in citizen–government relationships, as we have stated elsewhere (Taylor et al. 2009): some point to the development of a ‘Surveillance State’ as a result of the introduction of new digital IDM systems, whereas others perceive the emergence of a more effective ‘Service State’. We will describe each of these two emerging perspectives in more detail in section three.

Using characteristics of the presented informational trends and these two perspectives as heuristic tools, section four will report on empirical UK-based case study research, sponsored by the ESRC e-Society Programme. More specifically, the application and use of new IDM systems in three cases of public service relationships with the citizen will be described: a smart card application in local government, an online provisional driver’s licence application at the central administrative level and the deployment of Automated Number Plate Systems in policing services. Section five will further analyse these empirical findings for the ways in which ‘citizen identity information’ and ‘IDM’ have been reconceptualized in these case studies. Finally, in section six, the managerial, governance and democratic implications of managing citizen identity information in emerging e-government service relationships will be further discussed.

TRADITIONAL AND EMERGING FORMS OF MANAGING CITIZEN IDENTITY INFORMATION

Research shows that the management of citizen identity information in the public sector has known a long period of stability (Torpey 2000; Caplan and Torpey 2001; Pollitt 2009). Historically and archetypically in public service provision, citizen identification has been undertaken through manual form filling, often coupled to the submission of paper-based identification documents to the inspecting public official. In the past, government has established the exclusive right to issue and manage official citizen identification documents, such as the passport and driver’s licence. Moreover, the citizen registration service managed by government has confirmed individuals in their identity as citizens, giving all of them an official document recording their birth (Pollitt 2009). Citizen authentication too has been largely constant over time: for instance, the individual shows his or her official identification document to the public official
recognized to check and verify that the document carrier is the person referred to in
the document, aided in some instances by a photograph. Within this archetype of
citizen IDM, public organizations delivering services to the citizen have become vast
repositories of stored paper records including identity information on the citizen. So far
however we can observe that human assessment by public officials has been the decisive
factor in the management of citizen identity information (Lips et al. 2009).

Traditionally in public service arrangements, each individual who can represent
herself as an ‘authenticated’ and therefore legitimately acknowledged ‘citizen’ is
entitled to public service access. Moreover, all individuals who can legitimately claim to
be citizens of the State equally share the rights and responsibilities of citizenship (Faulks
2000). Citizenship identity therefore endows that citizen with equal status in public
service arrangements through the constitutional principle of equality under ‘the rule of
law’. Over time, systems have been created to store and retrieve records about an
individual’s public service eligibility, leading to the emergence of generic categories of
identity information on the individual: familiar personal details, such as name, address
and date of birth.

In the past, together with the expansion of the modern state, more specific public
service-related categories of citizen identity information have been introduced, such as a
National Insurance number, a National Health Number, student numbers or benefit
application numbers. Both these generic and specific identity information categories
have been acknowledged by government agencies as authoritative sources of citizen
identity information, usually supported by, or collected from, identification documents
issued by government. Usually, a separate citizen ‘identity’ has been constructed,
managed and used for each of the service relationships that the citizen has with
government agencies. For example, simultaneously and in parallel, the citizen has an
Inland Revenue taxpayer’s identity, a Health Service patient identity and a Social
Security identity as a contributor or claimant within the system. Together with this
development, governments in many countries have created separate public registers for
managing identity information related to a specific citizen identity. As a result, as each
of these service relationships between citizens and government agencies is supported
by a form of citizen identification, citizen IDM systems available to government in
traditional public service arrangements usually involve a patchwork of different, and
sometimes incompatible, means and approaches (Fishenden 2005).

This fragmented status quo of citizen IDM across government may be overcome as
governments introduce new digital IDM systems into their public service relationships
with citizens. These new forms of IDM are being managed and used to supplement, and
sometimes to replace, traditional forms of citizen identification, authentication and
registration. Although to this point little empirical evidence has been available about
how digital citizen IDM solutions are used when compared to citizen IDM in paper-
based public service relationships, prima facie it seems that the introduction of these
new means of identification in public service provision with citizens will lead to a
marked disjuncture from that earlier period.
While IDM is a relatively new term and its meaning not entirely settled (Bamford 2007; Oxford Internet Institute 2007), broadly accepted definitions of key IDM processes indicate that digital citizen IDM takes place on a different footing then we have been used to in the past. For instance, commonly used definitions of ‘digital identification’ as the association of information items (or ‘identifiers’) with a particular human being (Clarke 1994; Harper 2006), and ‘digital authentication’ as the process of checking an information claim or assertion made by the person about their identity, ensuring the person is the individual he or she claims to be (Crompton 2004; Greenwood 2007) demonstrate that ‘digital citizen IDM’ allows for an informational relationship that is remote and electronic rather than face-to-face or paper-based (Lips et al. 2006a). In general, the following changes to informational relationships are observed as a result of introducing digital IDM systems in e-government service environments (Camp 2003; Marx 2004):

- information can flow freely and in ways that are difficult to trace, compared to information in face-to-face and paper-based transactions within the confines of a physical locale and relatively closed networks;
- information can be copied and stored at almost no expense;
- an increased merging of previously compartmentalized identity information on the citizen;
- transactions become information dependent, with current identification systems relying on the confirmation of an individual’s information;
- transactional histories become more detailed and easily available to many;
- trust depends on transactional history reports rather than on personal recognition; and
- an increased blurring of lines between public and private places makes citizen identity information more publicly available.

These changes to informational relationships raise several fundamental questions and dilemmas for governments in redesigning public service relationships by introducing digital IDM systems.

For example, an individual’s ability to remain unidentified has declined significantly in IDM enabled e-government service relationships, causing deep concerns about an individual’s informational privacy protection for instance (FIDIS 2006). At the same time however we observe an increased freedom of choice for individuals to represent themselves, such as the use of different types of pseudonyms (e.g. email-address, fake name) in interactions with others including government agencies. A related issue is new opportunities to access, copy and abuse someone else’s informational details presented in e-government service transactions in order to get certain benefits. Acknowledging occurrences of ‘identity theft’ as a crime, many governments have enacted laws to deal with this new phenomenon.

A further example is the use of shared, matched or merged identity information on the citizen in order to provide new ‘personalized’ or integrated public services to
individuals (Dunleavy et al. 2006; Lips et al. 2006b). With these new opportunities for public service provision, an important dilemma for governments is how to manage a potential tension between policy goals of better co-ordinated or integrated public services to individuals in a customer-focused way, requiring more extensive data sharing, while protecting fundamental citizen rights like the individual’s privacy (6 et al. 2005; Bellamy et al. 2005). As new digital IDM offers possibilities to make use of citizens’ identity information in new ways, including for tasks that are far removed from the purposes for which personal data were originally collected, they may cause conflict with data protection regulations (6 et al. 2005; Bellamy et al. 2005; FIDIS 2006; Halperin and Backhouse 2008).

A further example is the possibility that collected identity information on the individual can be securely stored in a government database which can then be accessed by government officials or third party representatives to make copies from, match with other available data or run secondary data analysis. Put differently, a situation which usually is perceived as enhanced information security compared to identity information stored in paper-based files for instance, actually may lead to new security risks. A related example would be the availability of a back-up copy of a secure government database, which could be accessed by public servants or others and, for instance when stored on a memory stick, lost or stolen, as a range of recent Data Loss Incidents (DLIs) in the UK show.

Examples such as these suggest that new IDM-facilitated public service relationships between government and citizens require a deep reconsideration of citizens’ rights and responsibilities (Taylor et al. 2007).

IMPLICATIONS OF USING NEW IDM SYSTEMS: AN EMERGING SURVEILLANCE OR SERVICE STATE?

Based on the informational trends mentioned above, several scholars point at fundamental changes which may happen to informational relationships between the citizen and the State as a result of the application and use of new digital IDM systems. Interestingly however, scholars seem to have almost opposite views on the direction and outcomes of these fundamental changes as we have shown elsewhere (Taylor et al. 2009). Some scholars perceive fundamental changes happening as a result of a developing surveillance society in which government uses digital IDM systems as surveillance systems with a substantial impact on democratic citizen rights (e.g. LSE 2005; Murakami-Wood et al. 2006); others point at IDM-enabled innovation in public service provision to citizens, offering governments the opportunity to break down ‘vertical’ government silos and deliver integrated, more effective public services which meet the holistic needs of the citizen (Dunleavy et al. 2006). Each of these contradictory perspectives is shared and further supported by a varying group of UK government representatives. We will describe these two emerging perspectives of the ‘Surveillance
State’ and the ‘Service State’, respectively, in more detail below and present a comparative summary at the end of this section.

**Surveillance State perspective**

Several scholars have indicated that the introduction and use of newly available IDM systems is leading to substantial information imbalances in citizen–government relationships (e.g. Lyon 2001; LSE 2005; Murakami-Wood et al. 2006). Digital IDM systems are acknowledged as ‘surveillance systems’ which can monitor individuals’ behaviour as well as collect and process individuals’ identity information. Generally, surveillance is defined as ‘any collection and processing of personal data, for the purposes of influencing or managing those whose data have been garnered’ (Lyon 2001: 2). Similarly, acknowledging a development of increasing reliance on computer databases for surveillance activities, Clarke (1988, 1997) speaks about data surveillance or ‘dataveillance’, which he defines as ‘the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons’ (Clarke 1988).

Many scholars signal an emerging trend of surveillance ‘creeping’ into all aspects of society with profound implications for democratic citizen rights (e.g. Lyon 2006; Ogura 2006). For instance, a study produced by the academic Surveillance Studies Network points at developments in the UK where individuals’ daily lives are enveloped by massive surveillance systems. Available ICTs, such as mobile phones, CCTV cameras, satellites, radio-frequency identification (RFID) tags, Internet cookies and e-mail traffic, offer unprecedented automated ways to gather and process personal information of individuals: ‘where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance’ (Murakami-Wood et al. 2006).

As an outcome of rationalization practice in organizations, the use of digital IDM systems can support the modern state in its efforts to enhance speed, control and co-ordination (Murakami-Wood et al. 2006). Ogura (2006: 285) further explains that New Public Management ideas and models appear to be particularly amenable to using new surveillance systems, as the needs and behaviours of citizens, being perceived as customers, can be systematically monitored and translated into political marketing activities.

In general, several scholars point out that personal and group data captured by surveillance systems can be used to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion or access, for example (Lyon 2003a; Murakami-Wood et al. 2006). Consequently, surveillance systems are discriminatory technologies as they sieve and sort for the purpose of assessment thus affecting people’s life chances (Lyon 2003a: 20). However, surveillance does not proliferate just because of the availability of new IDM
systems: the development of surveillance is determined by the use of these IDM means by government or other organizations (Lyon 2001: 74).

As an example of dataveillance, in a recent effort to map and assess forty-six large centralized databases across UK Central Government departments, the authors of the Database State conclude that a quarter of the reviewed databases are almost certainly illegal under human rights or UK data protection law. Moreover, more than half of the reviewed databases have significant problems with privacy or effectiveness and could fall foul of a legal challenge. In summary, fewer than fifteen per cent of the assessed public databases are perceived to be effective, proportionate and necessary, with a proper legal basis for any privacy intrusions (Anderson et al. 2009: 4).

Scholarly viewpoints such as these are further supported by public statements of a variety of UK government representatives. For example, the UK Information Commissioner Richard Thomas signalled fears about the UK ‘sleep-walking into a surveillance society’ (BBC News 2006); in a June 2008 Speech on Security and Liberty, the UK Prime Minister emphasized the need to preserve individual liberties when introducing new ICT-enabled measures to fight crime and terrorism, such as those relating to identity cards, the National DNA Database and CCTV; and the UK House of Commons’ Home Affairs Committee called on the UK Government to give proper consideration to the risks associated with increasing surveillance in British society, as the resulting loss of privacy erodes trust and can change the nature of the relationship between citizen and state (House of Commons 2008). More recently, in 2009, the UK House of Lords’ Select Committee on the Constitution similarly concluded that, although the processing of personal data has always been part of public administration, there has been a profound and continuous expansion in the surveillance apparatus of the State (House of Lords 2009). In the view of this Select Committee, to respond to crime, combat the threat of terrorism and improve administrative efficiency, the development of surveillance and the collection and processing of personal information have become pervasive, routine and almost taken for granted in British society, with data being collected on the entire population and not just on traditional ‘suspects’. Consequently, the Select Committee observes a serious threat to principles of privacy and individual freedom as a result of the growing use of surveillance by government (House of Lords 2009: 9–10). Moreover, the selective way in which surveillance is sometimes used threatens to discriminate against certain categories of individuals (House of Lords 2009: 5).

**Service State perspective**

Many scholars point at a strong alignment between opportunities offered by newly available ICTs, such as new citizen IDM, and a New Public Management (NPM) style of reform (e.g. Hood 1991; Bellamy and Taylor 1998; Filipe Araújo 2001; Margetts 2003). Focused on improving the production and distribution of public services and
therefore supporting similar modernization aims to enhance customer-orientation and improve the quality of public services, some authors even ask themselves whether e-government and NPM programmes constitute a perfect marriage (Homburg 2004; Bekkers and Homburg 2005). In general, the quest for better co-ordinated, ‘joined up’ or more integrated forms of government have led to growing pressure for the sharing of citizens’ personal information among public service agencies (6 et al. 2005; Bellamy et al. 2005).

Due to newly available pervasive information-handling opportunities which can offer a response to emerging public sector problems resulting from NPM reforms, Dunleavy et al. (2006) point at the emergence of a new ‘Digital Era Governance model’. Newly available ICTs, such as digital IDM systems, not only support a transition to fully digital modes of operating for government agencies but also will bring about shifts in societal information-handling norms and patterns (Dunleavy et al. 2006). These authors characterize the emerging public management reform model under the following three themes (2006: 227–42):

- **Reintegration:** ICTs will put back together many of the functions and expertise clusters that NPM separated into single-function organizational units. Examples are the use of digital IDM systems to facilitate joined up government or to re-strengthen central processes in order to reduce duplication across government.
- **Needs-based holism:** ICTs will simplify and change the entire relationship between agencies and their clients, moving away from the NPM focus on business process management and towards a citizen- or needs-based foundation for organization. Examples are IDM-enabled public service reorganizations around a single client group or ask-once processes supported by reusing already collected citizen information.
- **Digitization changes:** electronic channels become the central feature of administrative and business processes. Examples are new forms of automated processes where no human intervention is needed in an administrative operation, such as electronic monitoring of customers (e.g. patients) or increasing transparency and offering citizens to track and self-monitor the processing of their service applications.

Recent UK policy developments similarly point at the importance of technology enabled ‘service transformation’. The UK Central Government Policy Strategy *Transformational Government – Enabled by Technology* (2005) for instance presents an agenda of three key transformations in the public sector: public services must be designed around the citizen and business; an increased culture of shared services to release efficiencies; and a broadening and deepening of government’s ICT professionalism. Similarly, a 2006 UK central government policy document points at the opportunities of using digital IDM systems for achieving effective public service transformation (Varney 2006). In presenting the now infamous Whitehall example of
how a bereaved UK citizen needs to address government service counters about forty-four different times, this report makes a clear case for further examining the scope for co-ordinating and integrating front-line service delivery to citizens and reducing the duplication of business processes in government, through the cross-government use of an IDM system. In that way, more holistic citizen-centric rather than narrowly focused customer-centric government may finally be achieved (Varney 2006).

Furthermore, political leaders in the UK have come to see ‘personalization’ as a new organization model for public service provision which can empower citizens as well as correct information asymmetries between service producer and consumer (e.g. Brown 2004; Reid 2004). ICT-facilitated personalized service provision is perceived as offering opportunities for establishing citizen-centric government and better maintaining traditional fundamental public service values, such as the equity value of universal service provision. In 2007, the UK Prime Minister’s Strategy Unit proposed to take further steps towards public service reform based on personalization over the next ten years (Prime Minister’s Strategy Unit 2007).

Based on the same informational trends described earlier, features of these two emerging perspectives on the Surveillance State and the Service State are summarized in Table 1.

**EMPIRICAL DATA ON THE USE OF DIGITAL IDM SYSTEMS IN PUBLIC SERVICE RELATIONSHIPS**

Despite the emergence of these two perspectives on the implications of introducing new digital IDM systems in service relationships between the individual and the State, it is interesting to observe that there is a dearth of empirical data on the actual use of these new systems in citizen–government relationships so far (Lips et al. 2009). Consequently, as the technology itself tells us nothing about the societal, governmental or managerial direction it will, or should be, taking, the extent to which unambiguous and coherent paradigms are emerging in contemporary public management seems to be a matter of interpretation (Hood 1998). However, despite the lack of empirically directed scholarly attention we are witnessing the application of digital identification means in many public service environments. What is also clear is that these technologies are being taken up in varying citizen–government relationships and in different institutional settings. Thus for instance, identity information on the citizen, captured both voluntarily and involuntarily, knowingly and unknowingly, is being collected, verified, managed and used within institutional arrangements ranging from single government agencies to more and less complex settings of multi-agency public administration and public–private partnerships.

In a two year research project, sponsored by the UK Economic and Social Research Council’s e-Society Programme, we chose to explore the application and utilization of a variety of emerging IDM systems in different public service domains and relationships.
with citizens, in an inductive way and using a social science perspective. In order to explore what is happening to citizen identity information capture, management, flow and assessments in government, we specifically focused on the managerial and governance dimensions of the application and use of new IDM systems in emerging e-government service relationships. Moreover, as this research project had no direct empirical antecedents, we were particularly interested in enabling deeper, broader and empirically informed understanding of the changing informational relationships between government and citizens enabled by new digital IDM systems.

We used case study research methodology in order to bring a depth of historical and contemporary understanding to our work that would enhance reliability, enrich our subsequent analysis and theoretical development, and enhance too the transferability to policy and practice of the research findings (Seale 1999). Each of these case studies involved an in-depth literature and policy document study; semi-structured interviews with key stakeholders involved in policy development and implementation at the UK central government level as well as with key individuals at both strategic and operational levels of the e-government service initiative under study. The selected case

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Surveillance State perspective</th>
<th>Service State perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Increased and systematic use of digital citizen IDM systems</td>
<td>Surveillance systems leading to rationalization and control</td>
<td>Public service support systems leading to service transformation</td>
</tr>
<tr>
<td>2. IDM objective</td>
<td>Risk management, ‘knowing the unknown’; increased efficiency</td>
<td>Targeted public service provision; customer relationship management; increased effectiveness</td>
</tr>
<tr>
<td>3. Purposeful attention to citizen identity information</td>
<td>Surveillance</td>
<td>Better public service provision</td>
</tr>
<tr>
<td>4. Increased information-sharing</td>
<td>Increased analysis; matching and merging of citizen identity information; profiling</td>
<td>Reduced duplication and fragmentation; joined-up government; integrated public service provision</td>
</tr>
<tr>
<td>5. Client focus</td>
<td>Monitoring; segmentation of service users; social sorting</td>
<td>Holistic needs-based service provision; personalization; citizen-centric government</td>
</tr>
<tr>
<td>6. Implications for citizen–government relationships</td>
<td>Increasing information asymmetries; eroding trust</td>
<td>Decreasing information asymmetries; increasing trust</td>
</tr>
<tr>
<td>7. Citizen rights’ implications</td>
<td>Violation of privacy and individual freedom rights</td>
<td>Improved access to public services; open government, transparency</td>
</tr>
</tbody>
</table>
studies are all in operation, each of them with a different primary ‘technological access point’ for the citizen to public services (e.g. Internet Portal, smart card, CCTV). Other variables designed into the study include different policy and service domains; differentiated institutional settings; and the sensitivity level to be attached to the capture and use of citizen identity information.

In this contribution we present three different empirical case studies in which a new digital IDM system is being used in a public service relationship with the citizen, and the implications this has for citizen identity information capture, management, flow and assessment. We used insights and perspectives from available academic literature as heuristic tools to explore inductively informational outcomes and implications of using different IDM systems in a variety of public service relationships and domains. To explore broadly and deeply the potential impact and implications of the use of new digital IDM in public service relationships with the citizen, we report on case studies where we can observe varying fundamental changes happening in information relationships between the individual and the State: a multi-functional smart card application in local government; an online provisional driver’s licence application at the central administrative level; and an Automated Number Plate Recognition system in policing services. We will first describe each of the case studies more in detail below.

Case Study 1: Smart card application in UK local government service provision

For a long time a UK local authority maintained separate public service relationships with citizens for various public service domains like library services, leisure services, public transport and education services. Within each of these public service relationships varying citizen identity information was collected and maintained on the basis of the information needs of the government agency involved. For example, under separate membership service agreements, library services would hold a library card number and leisure centre services a membership card number for each individual client besides generic citizen identity information like name, address and date of birth. Each of these local government service domains had its own citizen identification process based on checking an issued service-related membership card which, in the case of library services, also included an individual’s photograph.

In 1999, the UK local authority first introduced a ‘dumb’ loyalty flash card free to residents. Over 200 local retailers participated in the scheme, offering discounts for cardholders. In 2001, the loyalty card scheme was converted into a more extensive multi-functional smart card scheme. The multi-functional smart card is available on a voluntary basis and free of charge to those who live, work or visit the borough. In 2004, approximately 36,000 people out of a population of around 110,000 were holding a smart card; by 2006, an estimated 44,000 people had joined the local smart card scheme. From the introduction onwards, the local smart card scheme has had
continuing strong political support from the Conservative leader of the council. His original vision was to use smart cards for delivering concessionary travel services on public transport buses: as users would swipe their smart card before boarding, the council and bus companies would learn more about the travel habits of cardholders and determine the costs involved. However, despite continuing efforts and investigations, this particular smart card function has not been materialized so far.

The current smart card can be used for borrowing library books and making use of Internet facilities, accessing leisure centre facilities, paying for goods and services through an ‘e-purse’ function accessible across varying service domains, a cashless catering system in secondary schools across the borough, providing proof of age, providing proof of entitlement to concessionary bus travel and as a local retailers’ loyalty card. The smart card has a microprocessor chip and allows both contact and contact-less functionality. Each smart card (rather than each user) holds a sixteen digit smart card scheme wide unique serial number which can be scanned from the contact-less chip of the card. Card applicants need to provide generic citizen identity information, such as name, address, date of birth, telephone number, e-mail address, gender and ethnic group; moreover, further identity information is requested on senior citizenship, registered blind or partially sighted, and registered disabled. Each applicant is required to supply official documentary proof of name, signature and current address. For applicants under 16 years of age, a parent or guardian need to authorize the application by signing and providing full name, relationship to the applicant and address. All applicants are informed that the identity information they provide will be used for statistical and concessionary purposes as well as for planning and improving card services. Identity information may be shared with other public sector organizations where it is required by law and with other departments of the council where they are introducing future card applications and third parties working in partnership with the council to provide card services. Applicants are offered to opt out of information sharing or can withdraw their permission to share personal data at any time.

The multi-functional smart card scheme uses a central supplier database which holds a list of cardholders and their application details, along with basic card presentation data and e-purse data for those cardholders concerned. Moreover, the library service sector and the leisure service sector have their own information systems. An interviewee further explained to us:

for many years we have had a database holding personal information on our members, but we have never used it as management information. The fact that we now have a multi-functional smart card as a library membership card does not change anything in this situation: it is just a card, which happens to provide a member with access to our services.

Both the central supplier database and these sector-bound information systems are managed by private companies. The library service sector and the leisure service sector systems are linked, via the council’s network, to the central supplier database across
these two service sectors. For example, leisure services can be used by anyone anonymously but member benefits can only be enjoyed by smart card holders. In general, the UK Data Protection Act restricts the council from sharing data derived from smart card application and usage.

One of the public service uses of the smart card is a cashless catering system in four secondary schools across the borough. School pupils do not have to complete a smart card application form as schools hold all the relevant data. Cards are sent in bulk to the relevant schools instead of home addresses. Photographs are taken of pupils wearing school uniforms and cards are generated and issued to each pupil.

Pupils periodically load money onto the e-purse section of the card either using wall-mounted coin machines or through their parents submitting a cheque to the school’s administration office for staff to update accounts. They present their cards at the checkout in the canteen, where catering staff physically assess and match the photograph on the front of the smart card with the pupil and insert the card into a reader device that will automatically debit the correct amount from the e-purse. Pupils entitled to free school meals do not need to load money on to the e-purse, but present their card at the checkout in the same way.

Moreover, under a separate pilot project for extended smart card use, pupils swipe smart cards through a smart card reader at the beginning of each class. ‘Loyalty’ points are automatically accrued for every class attended. These points can then be supplemented with extra points for good behaviour, assigned at the discretion of teachers. Points are stored in the central supplier database and pupils are able to exchange them for goods and services with local retailers and organizations participating in the smart card loyalty scheme. Options for pupils include a free swim, cinema ticket or fast food meal. More recently, the UK local authority has been investigating the possibility of using the smart card to reward healthy eating by awarding loyalty points to pupils who buy approved food items for lunch. This may fit into an authority-wide ‘motivational scheme’ whereby positive behaviour, such as recycling, voluntary work and healthy lifestyles, is rewarded via smart card point accumulation.

Case Study 2: Online provisional driver’s licence application

UK citizens must apply for a provisional driver’s licence before taking a theory and practical test and upgrading to a full driver’s licence. Citizens wanting to apply for a provisional driver’s licence used to go to a local post office branch where they submitted a manually filled in form including demographic details, accompanied with paper-based proofs of identity. In the UK, there are approximately one million provisional driver’s licence applications a year.

Since April 2006, citizens are able to apply for a provisional driver’s licence via the UK central government’s ‘Direct.gov’ web portal and the UK central government’s authentication infrastructure, the so-called ‘Government Gateway’. If the customer
already has a Gateway log in (activation PIN) then he or she still has to register for UK Driver and Vehicle Licensing Agency (DVLA) services. Applicants who wish to hold a licence to allow them to learn to drive and take a driving test can complete an online form giving basic demographic details, such as surname, initials, date of birth and driver number if known, including three year address history.

First, the identity information on the submitted online form is electronically matched with the DVLA’s own database to retrieve any existing details for the applicant, including previous applications and driving disqualification information. If this data matching process brings forth no matches then the applicant can continue and a new record will be created. Equally, the applicant can proceed if one match is found (thus the applicant has been positively identified in the DVLA database) and these records do not preclude progression. However, if multiple matches occur this application will need manual checking and may not be able to be completed online. This might happen if the applicant has a common name or if duplicate records are held in the DVLA database for instance.

In the case where the applicant can proceed, the demographic identity information is automatically transferred via a data link to an external information solutions company. Using name and address history in particular, the external information solutions company employs search technology to match applicant data with a variety of public and private databases. This process assesses the applicant’s digital ‘footprint’ to seek assurance that the submitted name and address are bona fide and provides the DVLA with a software generated score which determines whether the application can be completed online. The generated trust score not only is based on the number of ‘hits’ produced but also on the quality of hits. For example, hits against mail-order catalogue databases likely produce a lower score than successful hits in banking databases. This is because banks are likely to have applied more authentication procedures to its customers than mail-order companies.

If the applicant fails the digital footprint assessment he or she will be provided with an on screen message instructing them to finish the process in the conventional paper-based format, for instance by sending an application form supported by official identity documents to the DVLA by post, often via a visit to a branch of the post office. If the applicant progresses through the footprint assessment, he or she will be asked to submit certain medical details (e.g. eye problems, psychiatric disorders, cardiovascular problems, neurological disorders or epilepsy) and passport number online. Using this number, the UK Identity and Passport Service will electronically transfer the applicant’s passport photograph and signature to the DVLA from digital passport records for use on the provisional driver’s licence. The applicant will then proceed to online payments using a credit or debit card and will also be able to check through all the provisional driver’s licence information details on a verification screen. Applicants are permitted to use alternative paper-based proof of identity documentation, such as their birth certificate, and can choose to use an alternative photograph. For each of these options, however, the application has to be completed offline.
Case Study 3: Automatic Number Plate Recognition (ANPR) in policing services

Police men used to stop suspect vehicles on the basis of their own professional judgement, conducting a driver’s licence check and using face-to-face authentication methods. Since 2003 our case study police force has employed UK Home Office provided Automatic Number Plate Recognition (ANPR) cameras, mounted in police vans and patrol vehicles, to read number plates of passing vehicles. An important motivation for using these cameras is provided by Home Office research showing that those who have committed traffic or vehicle-related offences are significantly more likely to have committed mainstream criminal offences than other road users (Rose 2000). Moreover, the police apply the basic intelligence principle that criminals use vehicles for committing a crime and are vulnerable on public roads therefore.

A thirteen month pilot scheme between 2003 and 2004 indeed found a fivefold increase in the arrest rate for frontline police officers when they had access to ANPR cameras (Connor 2005).

The ANPR cameras are mounted at both the front and rear of the vehicle and are able to read up to 3,000 Vehicle Registration Marks (VRMs) an hour for vehicles travelling up to 100 miles per hour. While the front camera has normal colour image capabilities, the rear camera is fitted with infrared; the latter is more effective at reading number plates (e.g. if they are dirty or obscured) while the former is required to show the colour of the car. Number plate information is then matched against a number of datasets in an attempt to detect and reduce crimes and misdemeanours. The case study police force has enlarged the scope of its initial activities through connection to existing local authority CCTV systems and other networks, such as that of the UK Highways Agency. They were also talking to the commercial sector about connection to their sites, particularly garage forecourts (Connor 2005). In December 2005, more than fifty local authorities had already signed up to the national ANPR scheme to allow the police access to data gathered from their CCTV traffic cameras. An interviewee further explained to us: ‘We are not Big Brother: we are only using available means of IDM to improve both the efficiency and effectiveness of our public service.’

Furthermore, the Association of Chief Police Officers announced plans in 2005 to develop a National ANPR Data Centre (NADC) to centralize all ANPR data from the forty-three police forces in England and Wales (although not from the London congestion charge scheme). In July 2009, the NADC was under development with a small number of police forces having access in order to help test the facility. In general, access to the NADC by UK police forces will be subject to the signing of a Memorandum of Understanding, setting out their responsibilities, including agreeing that access to data is solely for policing purposes, as defined within the code of practice on the management of police information under the terms of the Police Act 1996, in support of investigation. The NADC has around nine million plate ‘reads’ a day.
initially, with the capacity for fifty million a day. For every read, a photo of the number plate or ‘plate patch’ is also stored as a check (Mathieson 2007). Reads are kept for at least two years, both at the NADC and by the police force concerned, and can be used as corroborative evidence in court. ANPR data are treated as personal data under the UK Data Protection Legislation.

The ANPR technology aims to be ninety-five per cent reliable for UK number plates, although this falls slightly in adverse weather conditions and with foreign plates (Mathieson 2007). The system relies on access to a variety of public and private sector databases, such as those held by the DVLA (vehicles without a valid tax disc or with unlawful number plates; disqualified drivers, etc.), the Police National Computer (PNC) (lost or stolen vehicles; drivers of interest to the police), the Motor Insurance Database (uninsured drivers) and the Vehicle & Operator Services Agency (vehicles without a valid MoT test certificate) (Connor 2005). Patrol vehicles do not have a direct link to the PNC or to the police force’s control room. Rather, the on-board ANPR computers have data from these sources periodically loaded onto them. ‘Hits’ flash onto the screen real-time showing colour coded matches in the various databases used, which connect vehicles on the road with potential crimes and discrepancies. The hit rate is reported as less than two per cent, thus most vehicles pass through the camera systems without any action being taken; however the NADC will collect and store both ‘hits’ and ‘non-hits’ from police forces for designated periods of time. Furthermore, the NADC will allow analysis that has been difficult to do across police force boundaries, and carry out automated data-mining including a search for cloned vehicles on the basis of ‘impossibly quick journeys’ (Mathieson 2007).

Once a hit occurs, officers in the case study police force make a professional judgement about whether to pursue the vehicle. This pursuit is most likely to occur where more than one hit has occurred across the multiple databases involved. In addition to this reactive aspect of ANPR the system employed allows for proactive investigation of a vehicle through its VRM. If, during the course of patrols, officers spot what they consider to be a potentially suspect vehicle, they can deliberately position the camera equipment so as to take a reading from that vehicle. The equipment also permits officers to key in the VRM of a car they suspect but are not able to capture through the camera. Furthermore, staff in the police force control room can radio a VRM of particular importance so that officers can monitor the vehicle’s passage through the system.

Where there is prima facie evidence of an offence an officer takes one of two courses of action: officers may take the suspect to the local police station for formal identification and further questioning or charging. Alternatively, police officers may award a fixed penalty notice for offences deemed minor. Interviewed police officers indicate that ANPR methods may be fairer compared to pre-existing ‘suss’ techniques used by patrol police to apprehend and question suspects in vehicles: ANPR facilitates stops and searches based on ICT-mediated empirical evidence rather than postulations which may be a consequence of human prejudice (e.g. race, social class).
Looking at these empirical descriptions it becomes clear that the introduction and use of digital IDM systems in public service relationships has had a substantial impact on informational relationships between the individual and the State. In general, the organization and implementation of public service provision have become more information dependent and remote from the client compared to traditional paper-based or face-to-face public service environments. More specifically, we can observe several of the IDM enabled informational trends presented in academic literature across the three case studies.

For instance, compared to traditional public service relationships in which generic personal data, such as name, address or date of birth, are the primary sources of citizen identity information, the empirical case descriptions point to the emergence of varying alternative citizen identity information resources, such as a car licence plate number, a smart card unique serial number or a PIN. In the smart card application and the ANPR case studies surrogate citizen identity information not only is used alongside conventional identity information categories but also replacing these conventional categories as the more important identity information on the citizen.

Moreover, new identity information on the citizen is being generated and used in public service relationships enabled by digital IDM systems: for example, in the smart card application case, loyalty points for healthy eating or class attendance are allocated to pupils; in the provisional driver’s licence application case study, a digital footprint is generated based on a citizen’s presence in various government and private sector databases; and in the ANPR case study, number plate reads are generated and stored, and can be used for further analysis or as corroborative evidence in court. The latter example also points at the ease of storage of new identity information and the acknowledged opportunities for keeping these data for later analysis.

Furthermore, all three case study descriptions demonstrate that trust in these emerging e-government service relationships increasingly depends on data sets available in ‘trusted’ databases to which an individual’s identity information can be linked or matched, rather than on personal recognition. Moreover, not only databases created by and belonging to public sector organizations are being used in these service relationships but also databases from private sector organizations. Another informational trend recognizable across these case studies is an increased merging of previously compartmentalized identity information: for example, in the case of the multifunctional smart card, with the newly created central database containing cardholders’ identity information and e-purse data; the provisional driver’s licence application with the creation of an applicant’s digital footprint across a variety of public and private sector databases; and the ANPR case study with the development of a National ANPR Data Centre. However, the three empirical case study descriptions also demonstrate that citizen identity information is not flowing freely across public and private sector
organizations involved in a public service initiative, nor is there a strong development towards merging compartmentalized identity information, with many of the databases in use restricted to a specific public service domain or relationship.

Empirical observations such as these indicate that the management of citizen identity information is changing as a result of using digital IDM systems in public service relationships. From a citizen’s point of view for instance, manual form filling or presenting paper-based official identity documents and other proofs of identity become increasingly superfluous. Simultaneously, to the public servant, the management and use of large collections of paper-based documents stored in a personal file related to a particular client may increasingly belong to the past. Indeed there seems to be a development towards digital ‘joint spaces’ where service providers meet and assess their customers, as demonstrated for instance in the three case descriptions above. However, although computer-based assessments are increasingly playing an important part in public service relationships, final assessments on public service access and forms of public service provision continue to be made by public servants. In two of the three case studies, this final assessment is being restricted by determining the ‘bandwidth’ within which the system is allowed to serve the citizen automatically, such as in the smart card-related loyalty card scheme and the trust score assessment in the provisional driver’s licence case.

Another important change as a result of deploying digital IDM systems in public service relationships is that government is not the sole responsible party for managing citizen identity information any longer, as it used to be in traditional public service provision. Instead we can observe the introduction of what we call ‘third party authentication’ in emerging e-government service relationships with the citizen (Lips et al. 2009). Private sector organizations, such as the information solutions company in the provisional driver’s licence application case, are involved in verifying and authenticating citizen identity information. Subsequently, these organizations assess and construct a digital footprint of the citizen, which then constitute the basis for setting an individual’s trust profile. This trust profile determines whether an individual will be granted online access to public services or not. A further example of new public–private partnerships in the area of citizen identity management can be found in the smart card application case. There, the production and issuing of smart cards, as well as the management and maintenance of identity information collected through citizens using the smart card for a variety of public services, are responsibilities of a private sector company.

**MANAGERIAL, GOVERNANCE AND DEMOCRATIC IMPLICATIONS OF NEW FORMS OF CITIZEN IDM**

If we compare the empirical case study descriptions with the two emerging perspectives of the Surveillance State and the Service State, respectively, we can observe that there is
no particular perspective dominating in our empirical observations: characteristics of both perspectives are visible in these case studies simultaneously and in parallel, albeit within the legal restrictions of UK data protection legislation and not violating a citizen’s privacy rights or individual freedom so far. For example, Customer Relationship Management (CRM) has become an important strategy for our interviewees in the smart card application case study to develop further more effective, tailor-made public service relationships with established ‘loyal’ customers across a range of public services. At the same time, these targeted forms of public service provision can lead to improved risk management, control and increased efficiency, which for instance can be observed in the assignment of loyalty points for ‘good’ behaviour to these customers. Similarly, convenient online access to provisional driver’s licence services can only be granted to ‘trusted’ customers who have been monitored, socially sorted and segmented on the basis of their behaviour in other public and private sector service relationships. Or, in the case of using ANPR systems in policing services, a substantially improved public service provision including a fivefold increase in the arrest rate and professional assessments based on IDM-enabled empirical ‘evidence’ rather than human assumptions, can only be achieved as a result of surveillance, the matching of citizen identity information and increased analysis.

Consequently, in these emerging e-government service relationships, we can observe that the management of access to improved, customer-focused public services goes hand in hand with risk management. At the same time however, our interviewees explicitly aimed at meeting the characteristics of the Service State perspective and not belonging to the Surveillance State perspective therefore. For example, in the ANPR case study, available digital IDM systems were utilized only for the purpose of increased effectiveness and efficiency in public service provision and not for the purpose of monitoring individuals. Equally, in the smart card case study, although a digital IDM system was used across public services and public service organizations, public service-related information flows between the individual and government remained within a single public service domain – as in the traditional public service environment.

New forms of citizen IDM in public service relationships also have governance implications. Compared to the historical circumstances of government having the exclusive right to manage citizen identity information, we can observe that government is not the sole party for governing and managing IDM any longer. Public–private partnerships are emerging in various ways in all three case studies presented above, in most situations without any knowledge of the citizen-customer. The fact that access rights to public services can be decided upon by private sector companies rather than government (e.g. in the case of the provisional driver’s licence application), raises fundamental issues with regard to meeting traditional public service principles, such as equality under the law and universal access rights.

More fundamentally even, due to the use of digital IDM, citizen–government relationships appear to be changing in new directions, moving away from traditional conceptions of citizenship. In more general terms we may recognize a gradual shift from
universally applied principles in public service provision, such as administrative equity, to what may be called ‘particularism’ as an underlying conception of citizenship in emerging e-government service relationships. This development particularly manifests itself when the citizen is more and more being served as a unique customer of government. An individual citizen, who, due to good behaviour in using public services, receives loyalty points on his smart card for spending on local retail products, is a good example of an increasingly particularistic understanding of citizenship. With this gradual shift from universalistic to particularistic public service provision we are therefore moving away in some instances at least from universal access rights or democratic governance and participation rights, and towards more individually based public service arrangements between the individual and the State.

Moreover, newly gained identity information on the citizen can be used by governments for providing incentives to loyal customers, which will lead to preferred citizen behaviour. The use of digital IDM means as new steering instruments for paternalistic governments appears to be a much more active and interventionist management role of government in managing citizen identity information compared to the past where governments predominantly displayed passive behaviour in their responsibility for issuing identification documents and managing compliance regarding the citizen’s use of these documents (see for instance Torpey 2000).

Consequently, the newly emerging conception of ‘citizenship’ based on citizen identity information and the management of that information, which more and more is taking place in combined public and private sector realms and targeting on establishing new relationships with ‘loyal’ customers, suggests the need for fundamental rethinking of the role of government and its use of newly available IDM systems in public service relationships with citizens.

NOTE
1 PM’s speech on Security and Liberty, 17 June 2008. Available at http://www.number10.gov.uk/Page15785

REFERENCES


