IDENTITY MANAGEMENT, ADMINISTRATIVE SORTING AND CITIZENSHIP IN NEW MODES OF GOVERNMENT

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

[a] School of Information Management & School of Government, Victoria University of Wellington, Wellington, New Zealand [b] Oxford Internet Institute, University of Oxford, Oxford, UK

PLEASE SCROLL DOWN FOR ARTICLE

A. Miriam B. Lips, John A. Taylor & Joe Organ

IDENTITY MANAGEMENT, ADMINISTRATIVE SORTING AND CITIZENSHIP IN NEW MODES OF GOVERNMENT

In many countries, the introduction of new forms of identity management (IDM) in government, such as identity cards, smart cards or web-based e-authentication solutions, is receiving a lot of attention. Critics of these initiatives generally point at the expected outcome of substantial information imbalances between government and citizens. Clearly, newly formed, ICT-facilitated information relationships between government and citizens would not only need a reorganization of the e-government service domain itself but also a reconsideration of citizens' rights and responsibilities. However, to be able to address these issues adequately, we first need to gain further empirical understanding about what changes are happening to information relationships between citizens and government as a result of the introduction of new forms of IDM in e-government service provision. So far however there is not much empirical knowledge available about what changes are occurring both within and to these flows of information in new e-government service relationships between citizens and government. Accompanying these changes, important questions arise as to how, and to what extent, new forms of IDM have an effect upon what may be called the 'administrative sorting' activities of governments: those classifying processes caused by administrative systems and depending on the values embedded in those systems, which are necessary to the establishment of service relationships with citizens. What, then, are the effects on the citizen of administrative sorting in digitized service relationships, when set against the traditional concept of citizenship? This article reports on empirical findings derived from case study research on new forms of IDM in UK e-government. Moreover it seeks to conceptualize 'administrative sorting' and 'IDM' in e-government service relationships with citizens, also compared to traditional forms of IDM in the 'paper-based era' of public service provision, and explores what the implications are for the citizen and citizenship.

Routledge
Taylor & Francis Group

1.   Introduction

Governments throughout the world are introducing digitized personal identification and authentication systems into their service relationships with citizens (Accenture 2006). These new forms of identity management (IDM) are being managed and used in addition to, and increasingly to replace, traditional forms of personal identification and authentication. Digitized IDM systems not only appear to enable the modernization of government; they are also seen as enabling government to improve its service-providing functions to the citizen. For instance, they are purported to offer enhanced customer convenience; citizen mobility, empowerment and trust; efficiency and effectiveness of public service provision, including joined-up government; and public safety and security, including law enforcement. It is clear too that IDM increasingly belongs to the core of national and international e-government policy agendas (EU Ministerial Declaration on E-Government 2005).

It seems likely that the introduction, management and use of digitized IDM in citizen–government relationships will bring about changes at the operational level of public service provision to citizens. Many governments now perceive these newly available means of identification as the *sine qua non* for establishing the next stage in the evolution of e-government, i.e. transactional services between citizens and governments (Lips 2007). Moreover, robust IDM is perceived as helping to mobilize the uptake of e-government services which, as for instance recent UK uptake figures suggest, appears to be strongly needed (Dutton *et al.* 2005; Varney 2006).

Changes in the operation of public service delivery also imply changes in information relationships between citizens and governments. Scholars have pointed towards substantial information imbalances in citizen–government relationships that are a likely outcome of the introduction of these new means of IDM (LSE 2005; Murakami-Wood *et al.* 2006). Some perceive IDM systems as '*surveillance systems*', which, as a result of embedded codes and values, will bring about the '*social sorting*' of citizens: rationalized, automated processes of social classifications (Lyon 2001, 2003). Surveillance systems capture personal and group data in order to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, access, etc. (Lyon 2003, p. 20). Consequently, surveillance systems can be perceived as discriminatory technologies as they sieve and sort for the purpose of assessment, thus affecting people's life chances (Lyon 2003). Perceptions such as these suggest that new ICT-facilitated information relationships between government and citizens not only

require reorganization of the e-government service domain, but also, simul-taneously, a deep reconsideration of citizens' rights and responsibilities.

Compared with traditional paper-based citizen identification in public service provision, such as the submission of a passport or drivers licence as proof of identity, we now anticipate the introduction of new digitized forms of citizen identification, authentication and IDM influencing the design of service provision to the citizen. Accompanying this change, important questions arise as to how, and to what extent, these new forms of IDM have an effect upon what may be called the '*administrative sorting*' activities of governments: those classifying processes caused by administrative systems and depending on the values embedded in those systems, which are necessary to the establishment of service relationships with citizens. What, then, are the effects on the citizen of administrative sorting in digitized service relationships, when set against the traditional concept of citizenship?

To be able to address these questions adequately, we have sought stronger empirical evidence of changes to information relationships between citizens and government as a result of the transformation from a paper-based public service environment to an ICT-based public service environment. More specifi-cally, we have sought to focus on the implementation and use of new forms of IDM in these newly emerging e-government relationships. To this point little empirical evidence has been available about how these relationships are develop-ing, yet, when compared with personal identification and authentication in the 'paper-based era', *prima facie* it seems that IDM and the administrative sorting activities it supports will lead to a marked disjuncture from that earlier period.

To answer these questions in this article, we seek in the sections below to conceptualize 'IDM' and 'administrative sorting' and to explore their impli-cations for the citizen and citizenship.

2. What is IDM?

IDM has rapidly become a 'hot' concept in the private sector and increasingly in the public sector too (Birch 2007; FIDIS 2006; McKenzie *et al.* 2008; Socitm 2004; Sun 2004; Varney 2006). Technical solutions for identification processes in elec-tronic environments, such as 'federated IDM', the introduction of electronic ID cards or e-authentication solutions, are gaining much interest currently. What are seen as best practice examples, such as the Austrian Citizen Card initiative or the New Zealand e-authentication solution, are being presented at conferences around the world; with the New Zealand government recently collecting a global online identity award for its e-authentication programme (http://www.e.govt.nz/resources/news/2007/20070927.html).

Although IDM is as yet a far from settled concept it is mainly understood as comprising technical solutions to the problem of information security.

The former Australian Federal Data Protection Commissioner Malcolm Crompton, for instance, provisionally understands IDM as '*a set of data management systems and practices designed to increase confidence in the identity of individuals where appropriate*' (Crompton 2004, 2005). Another example can be found in the 2005 EU Ministerial E-Government Declaration: '*As our e-government services become more transactional, the need for secure electronic means of identification for use by people accessing public services is essential for citizen trust and in ensuring the effectiveness and efficiency of our public administrations*' (EU Ministerial Declaration on E-Government 2005, p. 5). The latter quote even shows that governments perceive technical security and citizen trust as intrinsic conditions fundamental to the effective delivery of e-government services. This citizen trust in government can be 'secured' by offering access to e-government services through secure means of electronic identification and authentication. Moreover these secure means of electronic identification and authentication would 'secure' citizens' trust in their experience of e-government services and, with that, lead to better results on e-government service take up figures.

Interestingly, and understandable perhaps because of its predominantly technical orientation, the introduction of digitized IDM has led to minimal public debate, though the UK national ID card has been one of the few exceptions to this rule. On those few occasions of public debate we observe that IDM moves from a narrow technical perspective to one focused upon the privacy rights of individuals. A common adage of privacy rights advocates looking at the introduction of new IDM systems is '*What can happen, will happen*'. If the technological capability exists then it will be used, thereby threatening the privacy rights of the individual. As an example, the declared aim of UK central government to introduce a national ID card containing up to three biometrics identifiers together with a National Identity Register acting as a central database in which details about individuals will be stored would in the view of privacy rights advocates unquestionably lead to government's use of the data including their sharing, sorting and matching opportunities that the technology makes possible. From this privacy perspective, the expected outcome of the UK ID card initiative is the all knowing state permanently looking through its '*glass customers*' or '*data subjects*' (Mayo 2005). More specifically, these new surveillance systems would increasingly lead to what Lyon (2001, 2003) calls the '*social sorting*' of citizens. Discriminatory sorting of citizens would occur depending on the values embedded in the specific computer codes used to process and classify citizens' personal data. As an example, Lyon argues that biometric ID cards, such as those promoted by the UK government, will permit sorting, profiling and discrimination in terms of ethnicity (Lyon *et al.* 2004).

These two different perspectives on IDM, the technical and the privacy rights perspectives, are largely sustained by *a priori* reasoning rather than by a clear empirically derived evidence base that casts light upon what is actually happening in different forms of e-government. Indeed there is a dearth of empirical data on the implementation and use of IDM systems in citizen–government relationships.

In a research project sponsored by the UK Economic and Social Research Council's e-Society Programme[1], we chose to explore the application and utilization of a variety of emerging IDM systems in different e-government service domains and relationships with citizens, from a social science perspective. In order to explore what is happening to new information capture, management, flow and assessments in government, we specifically focused on the policy and managerial dimensions of the application and use of IDM systems in 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 relationship between IDM systems and the nature of citizenship.

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 generalizability and transferability to policy and practice of the research findings (Seale 1999). For each of the case studies, we undertook an academic and policy document literature review to further inform us about the strategic and policy context, as well as c15 semi-structured interviews with key individuals at the operational, strategic and policy levels of managing identity in e-government service relationships. We also gained further insights on the strategic and policy context of IDM systems in e-government applications through semi-structured interviews with experts from the IDM industry and national policy makers in the field of IDM and/or e-government; two focus group meetings with policy makers and user group representatives, respectively; and an international-comparative IDM policy seminar with policy makers and experts from Canada, the USA and the UK.

Between February 2005 and March 2007, we conducted eight rich case studies across UK government, each of them having a different primary 'technological access point' for the citizen to e-government application areas where design and implementation choices about identification, authentication and IDM have already been made (e.g. Internet portal, smart card, CCTV). In so doing, we tried to gain further empirical understanding both of existing information capture, management, flow and assessment within a variety of e-government service relationships and upon information resources that are being sought as new digital relationships are forged. 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 personal information sensitivity. Table 1 below captures the distribution of case studies against these variables.

In this article we present some of the case-study findings from this work. Each of the case studies presented here is focused on practices to which we refer as 'administrative sorting'. In sections below we examine these sorting practices and compare them with practices from the traditional, paper-based public service world (Sections 5 and 6). Before we do so we provide a historical

TABLE 1 Case studies: organization, technology and the information nexus.

type of government organization	technological setting	type of information capture and management
1 Multi-level (central/local government) – social welfare	Face-to-face plus back-office ICT	'Heavy touch' personal data capture of benefits claimant including financial data. Data matching
2 Local government – leisure and learning services	Smart card	'Heavy touch' personal data capture. Basic smart card transaction data
3 Central Government – national healthcare call centres	Telephone	'Light touch' personal data capture. Medical symptoms and conditions data
4 Local Health Service – emergency treatment and transport	Mobile data communications	'Zero' to 'light touch' personal data capture contingent on medical condition. Patient symptoms and vital signs data
5 Central Government – probation service	Satellite monitoring	'Heavy touch' personal data capture. Location data
6 Police service	Mobile and fixed cameras	Vehicle information. Intense data matching. Personal identification
7 Executive agency – transport	Directgov Internet portal and Government Gateway	'Heavy touch' personal data capture and matching. Driver and vehicle information
8 Multi-level (central/local government) – education	Internet portal	'Light touch' personal data capture. Assessment, qualifications, learner development information

overview of the evolution of citizen identity and IDM in the paper-based era of
public administration.

3.   Emerging citizen identity, IDM and administrative sorting in the world of paper-based public service

During the twentieth century, we can observe a strong expansion of personal
identification practices in citizen–government relationships. The evolution of
social citizenship rights and entitlements, in particular, due to the expanding

welfare state after the Second World War, saw the number of separate public services provided to citizens expanded enormously, and a silo-structured' government with separate public counters for each citizen-facing government service domain emerge. Moreover, a further explanation offered for the expansion of personal identification practices aimed at establishing and verifying the citizen's identity has been the phenomenon of an increasingly mobile society. The movements of people had become less and less restricted to local or regional areas as they are likely to move across national borders. This increased international mobility of individuals led in turn to the establishment of a globally acknowledged, universal means of personal identification, the passport (Torpey 2000).

Normally, in paper-based public service a citizen would be permitted access to a certain service on the basis of manual form filling, the writing of letters and/ or the submission of official identification documents, such as the passport, drivers licence or birth certificate. Each individual who could represent him or herself as a legally acknowledged 'citizen' as a result of the authentication of his or her identification document(s) would be entitled to access a specific public service. Remarkably, this authentication process in identification practices has been largely constant: for instance, the passport holder continues to show his or her passport to the person officially recognized to check and verify that the document carrier is the person referred to in the document, aided in some instances by a photograph.

Moreover, legally acknowledged citizenship identity endowed a citizen with equal status in the paper-based public service world. Within the legal framework of post-war welfare states, this equal status of citizens has been recognized through the general administrative principle of 'equality under the law'. This general principle has been further translated into different forms of administrative equivalence of citizens in public service relationships as set out in Table 2.

In general, human assessment was the decisive factor in administrative sorting in paper-based public services: a public official would assess and decide

TABLE 2 Traditional principles of administrative equivalence in public service provision to citizens.

administrative equivalence principle	details
Access rights to services	Equal service access for all citizens within any particular governmental jurisdiction (national, regional, local, functional)
Procedure	Equal and fair treatment during the service process
Legal entitlement to a specific standard of service	Equal service outcome for similarly assessed cases, in accordance with legally embedded norms

upon an individual's paper-based request for access to a public service. Admin-istrative assessments arising from an individual's request to access a particular public service took place on the basis of a single set of administrative norms and values derived from the law and valid therefore within the governmental jurisdiction concerned. In cases where administrative norms left room for discretion, a civil servant would seek to apply existing administrative values based upon the notion of administrative equivalence as far as possible, e.g. through considering case law on the matter (Lipsky 1983; Snellen 1998).

Within this administrative system, a final assessment of a citizen's request for access to a public service could take considerable time. The various documents concerned were normally stored by the service-providing organization in a personal file as 'proof of entitlement' to the specific public service. In many cases citizens needed to queue until an official was able to bring one citizen's case to a close and start a new one.

Usually these personal files were kept for a certain legally acknowledged time period, again securing an element of administrative equivalence. Thus each individual service relationship was underpinned by a citizen's personal file and often attaching to that file was a unique case number. Public service providing organizations turned thereby into vast repositories of stored paper records containing different types of information related to a citizen's identity. Such information management was undertaken separately within each service-providing organization.

Enlarging paper-based regimes of citizen identification and representation in an increasing variety of administrative processes have introduced a central tension to IDM practices when compared with earlier identification practices based on 'face-to-face' identification. In the emergent world of documented identification a citizens' identity document had simultaneously become both a record of their uniqueness and an element in an administrative classification category that reduced the individual to a single unit in a statistical series (Caplan & Torpey 2001). Emerging from this document-based citizen–government relationship, a citizen did not fully own or control his or her personal administrative identity any longer. On the one hand an official document sustained personal identity and entitlements; on the other hand it became a data entity for the back-office of government and thereby amenable to forms of categorization, such as allowing access or not to a country or public services (Caplan & Torpey 2001; Noiriel 2001). Moreover systems were being created to store and retrieve information about an individual's eligibility, leading to the emergence of generic categories of identity – familiar personal details such as name, address and date of birth – made manageable through systems of unifying administrative numbers. We can also observe that these identi-fication categories increasingly became the basis for registering taxpayers, refugees, voters, schoolchildren and benefit claimants, to take some examples.

The representation of the citizen in identification and IDM practices thus developed into collective administrative, paper-based forms, such as a driver's

license or birth certificate, which could be used across a wide range of government services. At the intersection of individual and collective administrative identification systems, government and other public institutions had developed specific administrative methods for document-based citizen identification and authentication. Although citizen's identity documentation carried enabling as well as subordinating possibilities for citizens, it is interesting to observe that scholars, such as Weber (1968), emphasized only one side of the administrative 'identity equation'. The subordination or 'Big Brother' side of this equation, the checking and monitoring of targeted individuals for example quickly became dominant, doubtless given support from well-known historical examples of abuses of identification documents and population registers, such as the tracking of 'undesirable' populations in the Second World War. Early in this paper-based administrative era, therefore, a pejorative perspective was being attached by scholars to these administrative practices, one that would resonate with much later work on 'social sorting' (Burrows *et al.* 2005; Graham & Wood 2003; Lyon 2001, 2003).

4.   Exploring administrative sorting and IDM in new forms of e-government

What, then, happens to administrative sorting when new IDM systems are deployed in e-government service relationships with citizens? To what extent do these activities diverge from those administrative sorting practices and principles of the paper-based public service environment? A number of assumptions that inform answers to these questions are interesting to note here before we present observations from our empirical research.

First, we have seen that the technical orientation of new IDM systems predicts, as Crompton (2004) puts it, an increased confidence in the identity of individuals transacting with government. If this increased confidence is indeed an outcome of new IDM systems it can be expected to have an effect on the discretionary element in administrative sorting practices. A second assumption is that informational dimensions to a citizen's identity seem to become more complex and varied with the arrival of digital public service environments compared with paper-based environments. New forms of personal information may for instance be used in identification and authentication processes, such as a digitized biometric identifier, thus changing the basis of assessment of an individual's identity. Furthermore, the assessment and assignment of an individual's identity on the basis of a digitized biometric identifier may lead to forms of administrative discrimination based on eye or skin colour for example: the social sorting of citizens (Lyon 2001).

A third assumption is that as new opportunities for data linking and matching are taken up in the digital public service world, once more we can expect to see

new forms of administrative sorting. Snellen (1998) for instance foresees in citizen–government relationships the disappearance of the traditional 'street-level bureaucrat' exercising discretion, as, in his view the joining up of databases and the use of new information systems increasingly come to define the decision-making premises of street-level bureaucrats. Fourthly, Bovens and Zouridis (2002) point at the possibility of a shift in the discretionary space available for public officials as a result of newly available ICTs. In their view, as with Lyon (2003), these ICT systems will take over administrative sorting from human beings as decision algorithms are coded into the system itself. With that, discretionary powers within a public service providing organization do not disappear however. Rather, they are transferred to the designers of systems whose task is to transfer existing administrative rules, norms and values into system algorithms, codes and modules. Therefore, according to Bovens and Zouridis, it is these so-called 'system-level bureaucrats' who crucially interpret the will of lawmakers and create a formal set of decision rules through which categories of individuals will receive a certain service.

In presenting empirical findings gathered in four of our eight case studies we move beyond this largely *a priori* reasoning to explore how the concept of 'administrative sorting' can be understood in an electronic public service environment. For each of the case studies, after presenting a short introduction, we present empirical findings which demonstrate ways in which IDM and administrative sorting are taking place.

4.1   *Case study 1: smart card application in UK Local Government service provision*

In 2001 a UK Local Authority introduced a multi-functional smart card available free of charge to those who live, work or visit the borough. The smartcard can be used, for instance, to borrow library books, access leisure facilities, pay for goods and services, provide proof of age and prove entitlement to concessionary bus travel.

One of the public service uses of the smart card is a cashless catering system in four secondary schools across the borough. Here, pupils periodically load money onto an '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. Pupils present their cards at the check-out 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 onto 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 or positive behaviour, assigned at the discretion of teachers. The points are stored in a central database and pupils are able to exchange them for goods and services with local retailers and organizations participating in this loyalty scheme. Options for pupils include a free swim, cinema ticket or fast food meal. More recently the Authority has been investigating the possibility of using the smart card to reward healthy eating by awarding points to pupils who buy approved food items for lunch. Healthy eating points could be automatically accrued via the smart card and smart card readers at the check till and stored in a central database. 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.

4.2   Case study 2: online provisional drivers licence application

Since April 2006, citizens are able to apply for a provisional drivers licence via the UK central government's 'Direct.gov' web portal and 'Government Gateway' infrastructure. 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 including recent address history. Firstly, this information is electronically matched with the UK Central Government Department's own database to retrieve any existing details for the applicant, including previous applications and driving disqualification information. Secondly, the demographic information is automatically transferred via a data link to an external information solutions company that 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 UK Central Government Department with a software-generated score which determines whether the application can be completed online. If the applicant fails the footprint assessment, he or she will be provided with an on-screen message instructing them to finish the process in the conventional paper-based and face-to-face format, for instance by sending identity documents and other information to the UK Central Government Department by post.

If the applicant progresses through the footprint assessment, he or she will be asked to submit their passport number online. Using this number, the UK Identity and Passport Service will electronically transfer the applicant's passport photograph and signature to the UK Central Government Department from digital passport records for use on the provisional driving licence. Applicants are permitted to use alternative paper-based identity documentation, such as their birth certificate, and can choose to use an alternative photograph. For each of these cases, however, the application has to be completed offline.

4.3   *Case study 3: automatic number plate recognition in policing services*

For several years, an English police force has been using automatic number plate recognition (ANPR) cameras, mounted in police vans and patrol cars, to automatically scan and match car licence plate numbers in an effort to better detect and reduce crime. The main motivation for using ANPR cameras has been based on research evidence indicating that drivers who have committed traffic or vehicle offences are also likely to have committed mainstream criminal offences.

Activated ANPR cameras automatically seek to match licence plate numbers of passing vehicles with a variety of datasets held by UK Central Government Departments responsible for transport and vehicles, insurance industry, local police forces and in the Police National Computer, to identify those drivers and vehicles under suspicion for vehicular offences. Police officers engaged in ANPR operations are informed by in-vehicle monitors of matches or 'hits' in real time and are then able to apprehend the vehicle in question by dispatching a team of motorcycle police. Officers are permitted to use discretion in decisions about whether vehicles triggering a 'hit' are to be pursued. Questioning and searches may lead to the discovery of further criminal activity beyond those indicated by the automatic matching process. Licence plates appearing on several databases are perceived by police officers to be driven by those who habitually offend and may be associated with wider criminality.

Interviewed police officers indicate that ANPR methods may be fairer compared with 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).

4.4   *Case study 4: UK Local Government e-benefits system*

Since 2004 a local unitary council has been using an e-benefits system to assist citizens for housing and council tax benefits services. Previously, the claim would have been processed using a paper form submitted by the citizen and with potential support of front-office staff for filling in the form, which the back-office staff would have analysed later to provide a benefits calculation.

At present, a claimant is visited at home by a council officer who conducts an interview so as to be able to calculate and determine on the spot the levels of benefit that can be claimed. The officer uses a tablet PC that is loaded with specialized software; personal demographic details are taken as well as information regarding the claimants living arrangements, income, bank account details, saving, assets and other benefits claimed. By inputting this information into an on-screen form, the software is able to calculate the benefits that will be received. The claimant also has to show the officer several paper identity documents required for getting

access to benefits services, such as passport, drivers licence and payslips. Both the claimant and the officer sign the form using an electronic pen, as a claimant's signature is legally required to officially acknowledge the claim form. The officer's signature has been acknowledged at the central Ministry as enhancing the legal circumstances of a claim. The approved form is then sent via a wireless network as an email attachment to the council headquarters, and stored in a central database on the council's server, containing all approved local benefit claims.

The local council also exchanges benefits data of local benefit claimants with the UK Central Government Department of Work and Pensions (DWP). The council electronically transfers claimant information to the DWP; the DWP matches personal details of claimants with a variety of datasets held within its own information systems and those of the UK taxation agency. The matching process helps to provide indications that the claimant may be erroneously or fraudulently claiming benefits. This information is passed to the local council to act upon at its discretion. The DWP also runs ICT-supported intricate risk analysis, which places claimants into a risk category based on their individual profile. The Department attributes a risk score, which indicates the likelihood of error or fraud being associated with each category of claimant. This risk data is sent to the local council to follow up in its case-review schedules; council interventions based on high-risk scores can lead to the discovery of underpayments as well as overpayments to claimants, the consequence either of error or fraud.

5.   Analysis of administrative sorting and IDM in e-government service provision

5.1   *Changing administrative sorting practices*

It becomes clear from these case study findings that new forms of administrative sorting in e-government service provision are emerging compared with administrative sorting practices in traditional paper-based service provision. The smart card application in local government, where for instance loyalty points for class attendance are allocated automatically to pupils; the online provisional drivers licence application, in which citizen information is matched electronically with both government and private sector databases; ANPR in policing services, matching licence plate numbers with a variety of data sets; and the e-benefits system, where claimants are served at their homes are all examples of different administrative selection and assessment activities or administrative sorting practices, arising from the use of varying digitized IDM systems, in citizen–government relationships.

Interestingly in these new forms of administrative sorting in electronic public service environments, our research findings indicate that human, judgement-based assessments remain of substantial importance, in contrast to Bovens and Zouridis'

(2002) assertions. In most of our case studies, such as in all four presented above, final assessments on public service access and forms of public service provision continue to be made by civil servants. In some of the case studies, this final assessment is being restricted by determining the 'bandwidth' within which the system is allowed to serve the citizen automatically, as we have seen in those case-study findings on the loyalty scheme attached to using a local smart card and the digital footprint assessment during the online drivers licence application.

With that, we may observe that newly available IDM supports civil servants in their assessments and further decision-making in ways that lead to new forms of administrative sorting. First of all, we can observe that civil servants are being guided by digitized systems through the public service provision process, for instance utilizing pre-filled digital forms or standardized questionnaires in their service relationships with citizens. The e-benefits system mentioned above is a good example where a digitized system, based on various forms and pieces of personal information collected at the home of the benefits claimant, is able to calculate and determine on the spot the levels of benefit that can be claimed, bringing about changes in assessment and decision-making processes.

Secondly, support happens through the availability of improved knowledge to the civil servant in situations of assessment during public service provision. The so-called evidence-based public service provision and, more specifically, the newly based administrative sorting activities that derive from this approach can be observed, for instance, in the ANPR-case study mentioned above. Interestingly in this respect too, in contrast to Lyon's (2001, 2003) arguments, this particular case study demonstrates that newly available IDM systems do not need to bring about the social sorting of citizens. On the contrary, in this case new IDM supports civil servants in administrative sorting activities in ways that decrease human prejudice leading to more equitable decision-making regarding potential suspects. Put differently, evidence-based administrative sorting leads to higher-quality public service provision.

In those cases however, where evidence-based administrative sorting activities happen without the intervention of human beings, such as the ICT-supported risk analyses in the e-benefits system case or the digital footprint assessment in the online drivers licence application, Lyon's (2001, 2003) arguments do come to the force again. Although citizens in these cases are not sorted based on their *social* characteristics but on their 'loyalty profiles', in respect of specific public services or 'profiles of good behaviour', which can have direct implications for citizens in gaining access to public services.

5.2   *New types of personal information collected*

Within these changing administrative sorting practices, we also observe a shift towards the collection, management and use of new types of personal data. Compared with the paper-based public service world where 'traditional'

personal data such as name, address or date of birth are key personal identifiers for citizens, these empirical observations point to alternative and composite citizen identities, such as a car licence plate number, health number, email address, location data or a digital footprint based on a citizen's presence in various databases. As a result of new combinations of human and computer assessments (e.g. claims assessments in the e-benefits system, ANPR), compared for instance with personal data gathering in the paper-based public service word, hard and soft types of citizens' personal information have become more fluid categories. In the abstract, these new types of personal data can be perceived in concentric circles at varying distances from the individual's core identity (Marx 2003). What we also observe however is that these separable identities can become parts of a composite identity with public bodies seeking to confirm identity, thereby authenticating it, from among these various alternatives available in the digital world.

A further empirical finding, diverging from prevalent scholarly assumptions, emerged in several cases where we observed that it was unimportant to public servants whether they knew or not the citizen's name, address or other traditional personal data; more important to them was that they could serve that particular citizen on the basis of minimal personal information needed to establish the service; and serve him/her well – or even better, in case of a regular customer. Put differently, in several cases a citizen has a choice to remain anonymous, or use pseudonyms in their service relationship with government. In Health and Emergency Services, for example, there is little that may be termed administrative sorting occurring, as the traditional principles of administrative equivalence set out in Table 2 still pertain.

5.3   *Service values versus public safety values*

Emerging forms of administrative sorting also show us the importance of service values in these e-government relationships as distinct from public safety values and crude social-sorting activities. For example, customer relationship management (CRM) for many of our interviewees has become an important strategy for e-government to develop tailor-made service relationships with established customers. Newly available management information derived from ICT-supported interactions in the front-office or the back-office of e-government service provision opens up active and even pro-active opportunities for enhanced service provision to the citizen.

Some explanations coming from two of our interviewees further demonstrate these arguments. An interviewee in the ANPR case: '*We are not Big Brother; we are only using new means of IDM to improve both the efficiency and effectiveness of our public service*'. An interviewee in the local smart card case explained '*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*

multifunctional smart card as a 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'. Taking data-protection legislation into account as well as utilizing available digitized means only for the purpose of quality enhancement of a specific public service towards customers – not trying to profile customers by extending systems so as to include other databases or networks – were considered to be important conditions for service value compliance. Although in some cases newly available means of IDM were used across public services or public service organizations, such as in the smart card case or the application of a provisional drivers licence through the UK government's Direct.gov web portal and Government Gateway infrastructure, usually information flows between citizens and governments remained within a single public service domain – as in the traditional paper-based public service world.

5.4   *New public–private partnerships for citizen identification and authentication*

Another important indicator for change in administrative sorting activities in e-government is that government is not the sole responsible party for citizen identification and authentication any longer, as it used to be in the paper-based public service era. Instead we observe the introduction of what we call 'third party authentication' in e-government service relationships with the citizen. With restricted or even no knowledge of the citizen, private-sector organizations, such as the ones trusted by the UK government (see for instance the information solutions company in the online drivers licence application case), are involved in verifying and authenticating citizens' identity. These organizations then are assessing and constructing citizens' digital footprints, which then constitute the basis for setting an individual's trust profile. This trust profile determines whether or not an individual will be granted online access to public services.

A further example of new public–private partnerships in the area of citizen identification and authentication 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 personal information collected through citizens using the smart card for a variety of public services, are responsibilities of a private sector company.

6.   Implications for the citizen and citizenship

Research findings, such as those presented above, demonstrate that new representations of citizen identity, citizen identification and IDM in e-government service provision are effecting substantial changes in citizen–government relationships when compared with those in traditional paper-based service

environments. For example, the arrival of new IDM in e-government service provision may be shifting, from a citizen's point of view, to a system wherein paper-based public service characteristics, such as form filling, queuing and waiting, become increasingly superfluous. Simultaneously, to the civil servant, the collection, management and use of large collections of paper-based documents stored in a personal file that is related to a particular public service may increasingly belong to the past. Furthermore, there seems to be a development towards digitized 'joint spaces' where service providers meet and assess their customers, such as for instance the smart card application case and the online drivers licence application case, above.

More fundamentally, and consequent to the implementation and use of digitized IDM, citizen–government relationships appear to be changing in new directions, moving away from traditional conceptions of, and principles for, citizenship. Looking again at different forms of administrative equivalence of citizens served in paper-based public service environments (Table 2), we may observe that new administrative sorting practices in e-government service relationships, such as those presented above, are moving away from the application of these principles. From general principles of administrative equity we are moving towards differentiation in the selection and assessment of citizens. In more general terms we may recognize a gradual shift from 'universalism' to what may be called 'particularism' as an underlying conception of citizenship in an e-government service environment. This development particularly manifests itself when the citizen is more and more being administratively sorted in a 'vertical' way: as a unique customer of government, rather than a citizen with equal rights and duties compared with other citizens. 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.

Differentiation as a result of using digital IDM systems not only takes place vertically but also in horizontal ways. For instance, new administrative sorting practices, such as establishing conditional online access for trusted citizens only as in the online drivers licence application case, lead to new forms of citizen segmentation: those who can be trusted according to their digital footprint, and those who cannot. With that, the administrative sorting of customers and non-customers for e-government service provision, based on different trust profiles of citizens, in our view implies a new conception of citizenship: 'layered citizenship' is being established through 'horizontal', segmented administrative sorting of citizens (Taylor *et al.* 2007).

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 equal procedures and towards more individually based public-service arrangements between a citizen and government. Public service arrangements, increasingly based on varying types and combinations of information,

collected remotely or in face-to-face encounters, are held and used at the level of an individual citizen. Consequently, this newly emerging conception of 'citizenship' based on *individual* citizen identity and facilitated by new electronic modes of IDM, which is more and more taking place in combined public and private sector realms, suggests the need for fundamental rethinking of government's use of IDM and administrative sorting in its service relationships with citizens. With that, important societal questions emerge about the governance of IDM and IDM policy development in the digital state, both now and for the future.

Note

1   ESRC e-Society Project: Personal Identification and Identity Management in New Modes of e-Government. Ref: RES-341-25-0028.

References

Accenture (2006) *Leadership in Customer Service: Building the Trust*, [Online] Available at: http://www.accenture.com/Global/Services/By_Industry/Government_ and_Public_Service/PS_Global/R_and_I/BuildingtheTrustES.htm (28 April 2009).

Birch, D. G.W. (ed.) (2007) *Digital Identity Management: Perspectives on the Technological, Business and Social Implications*, Gower, Aldershot.

Bovens, M. & Zouridis, S. (2002) 'From street-level to system-level bureaucracies: how information and communication technology is transforming administrative discretion and constitutional control', *Public Administration Review*, vol. 62, no. 4, pp. 424–433.

Burrows, R., Ellison, N. & Woods, B. (2005) *Neighbourhoods on the Net: Internet-based Neighbourhood Information Systems and their Consequences*, The Policy Press, Bristol.

Caplan, J. & Torpey, J. (eds) (2001) 'Introduction', in *Documenting Individual Identity: the Development of State Practices in the Modern World*, Princeton University Press, pp. 1–12.

Crompton, M. (2004) 'Proof of ID required? Getting identity management right', *Paper Presented at the Australian IT Security Forum*, Sydney, 30 March 2004, [Online] Available at: http://www.privacy.gov.au/news/speeches/sp1_04p. html (28 April 2009).

Crompton, M. (2005) 'Trust, identity and connected government', Paper presented at the *Forum for the Research, Development and Evaluation Commission*, 'The evolution of e-government—from policy to practice', Taipei, 24 June 2005.

Dutton, W. H., di Gennaro, C. & Millwood Hargrave, A. (2005) *Oxford Internet Survey 2005 Report: The Internet in Britain*, [Online] Available at: http://www.oii.ox.ac. uk/research/publications.cfm (14 August 2008).

EU Ministerial Declaration on E-Government (2005), presented at ministerial e-government conference *Transforming Public Services*, Manchester, 24 November 2005.

FIDIS (2006) *Future of Identity in the Information Society: Identity in a Networked World – use Cases and Scenarios*, [Online] Available at: http://www.fidis.net/filead min/fidis/deliverables/fidis-wp2-del2.6_Identity_in_a_Networked_World.pdf (14 August 2008).

Graham, S. & Wood, D. (2003) 'Digitizing surveillance: categorization, space, inequality', *Critical Social Policy*, vol. 23, no. 2, pp. 227–248.

Lips, A. M. B. (2007) 'E-Government under construction: challenging traditional conceptions of citizenship', in *E-Government in Europe. Rebooting the State*, eds P. Nixon & V. Koutrakou, Routledge, London, pp. 33–47.

Lipsky, M. (1983) *Street-level Bureaucracy. Dilemmas of the Individual in Public Services*, Russell Sage Foundation, New York.

LSE (2005) *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, The LSE Identity Project Interim Report, March 2005.

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*, Open University Press, Buckingham.

Lyon, D. (2003) 'Surveillance as social sorting: computer codes and mobile bodies', in *Surveillance and Social Sorting: Privacy, Risk and Digital Discrimination*, ed. D. Lyon, Routledge, London, pp. 13–30.

Lyon, D., Combet, E. & Rule, J. B. (2004) 'Identity Cards: Social Sorting by Database', Oxford Internet Institute Internet Issue Brief No. 3, [Online] Available at: http://www.oii.ox.ac.uk/research/publications.cfm (14 August 2008).

Marx, G. T. (2003) 'Varieties of personal information as influences on attitudes toward surveillance', Paper prepared for a conference on the new politics of surveillance and visibility, [Online] Available at: http://web.mit.edu/ gtmarx/www/vancouver.html (14 August 2008).

Mayo, E. (2005) 'The age of identity', *Speech at the Foundation for Science and Technology*, London, February 2005.

McKenzie, R., Crompton, M. & Wallis, C. (2008) 'Use cases for identity manage-ment in e-government', *IEEE Security & Privacy*, vol. 6, no. 2, pp. 51–57.

Murakami-Wood, D., Ball, K., Lyon, D., Norris, C. & Raab, C. (2006) 'A report on the surveillance society', [Online] Available at: http://www.ico.gov.uk/ upload/documents/library/data_protection/practical_application/surveillance_ society_full_report_2006.pdf (14 August 2008).

Noiriel, G. (2001) 'The identification of the citizen: the birth of republican civil status in France', in *Documenting Individual Identity: The Development of State Practices in the Modern World*, eds J. Caplan & J. Torpey, Princeton University Press, pp. 28–48.

Seale, C. (1999) 'Quality in qualitative research', *Qualitative Inquiry*, vol. 5, no. 4, pp. 465–478.

Snellen, I. Th. M. (1998) 'Street level bureaucracy in an information age', in *Public Administration in an Information Age. A Handbook*, eds I. Th.M. Snellen & W. B. H. J. van de Donk, IOS Press, Amsterdam, pp. 497–505.

Socitm (2004) *Knock, Knock: Who's there? – an Overview of Authentication for Electronic Service Delivery*, Socitm, Northampton.

Sun (2004) 'Identity Management: Technology Cornerstone of the Virtual Enterprise', *White Paper*, [Online] Available at: http://www.sun.com/software/products/identity/wp_virtual_enterprise.pdf (14 August 2008).

Taylor, J. A., Lips, A. M. B. & Organ, J. (2007) 'Information-intensive government and the layering and sorting of citizenship', *Public Money & Management*, vol. 27, no. 2, pp. 161–164.

Torpey, J. (2000) *The Invention of the Passport: Surveillance, Citizenship and the State*, Cambridge University Press, Cambridge.

Varney, D. (2006) 'Service Transformation: A Better Service for Citizens and Businesses', *A Better Deal for the Taxpayer*, HSMO, London, [Online] Available at: http://www.hm-treasury.gov.uk/media/4/F/pbr06_varney_review.pdf (14 August 2008).

Weber, M. (1968) *Economy and Society: An Outline of Interpretive Sociology*, Bedminster Press, New York.

A. Miriam B. Lips is Professor of E-Government at Victoria University of Wellington, Wellington, and Research Associate at the Oxford Internet Institute, University of Oxford. *Address*: School of Information Management & School of Government, Victoria University of Wellington, PO Box 600, Pipitea Campus, Rm RH 812, Wellington, 6035, New Zealand. [email: miriam.lips@vuw.ac.nz]

John A. Taylor is Emeritus Professor of Government & Information Management at Caledonian Business School, Glasgow, and Research Associate at the Oxford Internet Institute, University of Oxford. *Address*: Oxford Internet Institute, University of Oxford, 1 St Giles, Oxford OX1 3JS, UK. [email: jta@gcal.ac.uk]

Joe Organ is Admissions Administrator at St Edmund Hall and a former Research Fellow at the Oxford Internet Institute, University of Oxford. *Address*: Oxford Internet Institute, University of Oxford, 1 St Giles, Oxford OX1 3JS, UK. [email: joe.organ@seh.ox.ac.uk]