Information Polity 15 (2010) 273–289
DOI 10.3233/IP-2010-0216
IOS Press

Rethinking citizen – government relationships in the age of digital identity: Insights from research

Miriam Lips
Victoria University of Wellington, PO Box 600, Wellington, New Zealand
Tel.: +64 4 463 7411 or 5507; Mobile: +64 27 563 7411; E-mail: miriam.lips@vuw.ac.nz

Abstract. The introduction and use of new ICT-enabled means of managing citizen identity information in public service environments may lead to fundamental changes of the informational foundations of citizen – government relationships. This raises important theoretical and empirical questions about the impact and implications of emerging information age government on the 'social contract' between the citizen and the State. To many scholars, it is clear that the introduction of ICT-enabled forms of managing citizen identity information at least requires fundamental rethinking around substantial 'contractual' issues, such as privacy and equity. Thus far however, there is little empirical evidence available of the changes happening to citizen – government relationships.

In this contribution, scholarly thinking around the impact and implications of the use of new digital forms of citizen identity management in public service environments is further explored. In particular, the development is explored of two seemingly opposite scholarly perspectives thus far: a Surveillance State perspective and a Service State perspective. This scholarly thinking is then confronted with empirical research findings. In so-doing, three substantive empirical research projects, one from the UK and two from New Zealand, are drawn upon. Two of these studies explored the management of citizen identity information from the perspective of government agencies in their public service relationships with citizens, whilst the third study explored the attitudes of citizens towards the management of personal information with and across government in the course of electronic public service provision. Finally, a meta-analysis of the empirical research findings and conclusions on changes in citizen – government relationships in the age of digital citizen identity is presented.

1. Introduction

Citizen identity information has become a critical underpinning of public service relationships between the citizen and the State. Over the years, in order to manage access to and consumption of a large variety of public services, governments have introduced generic categories of citizen identity information, such as name, address or date of birth; more specific service-related categories of citizen identity information, such as a National Health number, a student number or a Social Security Number; and officially recognised citizen identification documents, such as a passport, driver's licence or birth certificate. Usually, a separate citizen 'identity' is constructed, managed and used for each of the service relationships the citizen has with the public sector: for example, a citizen, simultaneously and in parallel, can have a health patient identity, a student identity and a benefit claimant identity [34,37].

These longstanding informational foundations of citizen – government relationships are being further extended as governments introduce new means of managing citizen identity information in public service environments. Now, a citizen no longer needs to engage with government via face-to-face contact or written communication, but instead can deal with public sector organisations purely on a 'remote' basis

1570-1255/10/$27.50 © 2010 – IOS Press and the authors. All rights reserved

through, for example, Internet-based provision of a large variety of public services, electronic toll roads or speed cameras, multifunctional smart cards for access to public services and buildings, electronic voting and other forms of ICT-enabled democratic engagement, and SMS messages in times of natural disasters. Moreover, these new informational exchanges between citizens and government are supported by the processing, storing and archiving of digitised data sets on the citizen, and the creation of digital public records.

These ICT-enabled developments in a wide range of public service environments raise important empirical questions about the impact of emerging information age government on the 'social contract' between the citizen and the State: does this reorganisation of informational relationships between citizens and government in public service arrangements lead to any fundamental changes in citizen – government relationships and, with that, to changes in existing roles and responsibilities of the citizen and the State in the management of citizen identity information? If so, what then are the implications of informational changes in ICT-enabled public service relationships between government and citizens?

The informational capabilities of the citizen identity management technologies that are being introduced in public service environments indicate the likelihood of fundamental changes happening to citizen – government relationships. For instance, several scholars point towards substantial information imbalances in relationships between the State and its citizens as a result of the introduction of these new 'surveillance systems' [41,50]. Some point out that the use of new citizen identity management systems is leading to the 'social sorting' of citizens: to the processing of captured personal and demographic data by government agencies in order to classify people, and determine who should be targeted for special treatment, scrutiny, eligibility, or exclusion, for example [44]. Perceptions such as these suggest a substantial impact on citizen rights and other citizenship-related entitlements: on privacy, equity, security, anonymity, or even on citizens' trust in government, to take some examples [2,5,9,16]. Others however indicate that the introduction of new citizen identity management systems will enable a new public management model which includes more effective public service provision to citizens [18]. Taking into account the needs of the citizen instead of those of government agencies, ICT-enabled holistic ways of public service provision may lead to empowerment, rather than subordination, of the citizen in her relationship with the State.

Thus far however, there is little empirical evidence available to support theoretical claims, such as those mentioned above. At the same time it is clear that the introduction of ICT-enabled forms of citizen identity information and citizen identification in public service environments at least requires fundamental rethinking around the emergent and complex issues, such as privacy, trust, equity, and effectiveness. In this contribution, scholarly thinking around emerging digital forms of citizen identity management in public service environments, and their implications for citizen – government relationships, is further explored. In particular, the development is explored of two seemingly opposite perspectives in scholarly thinking thus far: a Surveillance State perspective and a Service State perspective. This scholarly thinking is then confronted with empirical research findings. In so-doing, three substantive empirical research projects, one from the UK and two from New Zealand, with which the author has been directly involved, are drawn upon. The first two of these studies explore the collection, processing, storing, and use of citizen identity information from the perspective of government agencies in their public service relationships with citizens. The third of these studies was done in New Zealand and explored the attitudes of citizens[1] towards the disclosure, sharing and management of personal information with and across government in the course of electronic public service provision. Finally in this paper, a meta-analysis

[1]This citizenship notion includes individuals with New Zealand citizenship and those who are permanent resident.

of the research findings and conclusions on changes in citizen – government relationships in the age of digital identity is presented.

2. Emerging digital forms of citizen identity management in public service provision

For decades, and in some cases more than a century, the ways and forms in which citizen identity information have been collected and managed in public service environments in democratic countries, have been largely unchanged [13,36,55,60]. Typically, the management of citizen identity information in public service provision involves the need for the citizen to disclose personal details to government by filling in a paper-based form, supporting that form with officially recognised citizen identification documents, and submitting these paper-based documents to an official representing the service providing organisation. Usually, this public official not only authenticates the citizen by verifying that the person who submits the form is the same person referred to in the underlying identification documents, but would also assess an individual's identity information against generic public service criteria and paper-based records held on that individual within the public service organisation in order to decide on service eligibility. As a result, the assessments of paper-based forms of citizen identity information by the public official are critical in allowing individuals access to public services [36,57].

Commonly in public service provision, each individual who can represent herself as an 'authenticated' and therefore legitimately acknowledged 'citizen[2]' is entitled to public service access. Moreover, all individuals who can legitimately claim to be citizens of the State share the same rights and responsibilities of citizenship in accordance with administrative principles of equity under 'the rule of law' and fair treatment [19]. Furthermore, public service organisations have created their own files and registers for managing citizen identity information related to a specific public service relationship. In addition, many democratic countries have legislation in place to protect access to government-held records on a long term. This legislative requirement forces public service agencies to create and maintain public records, including citizen identity information, and to retain them for as long as required [33].

As a result, as each public service relationship between citizens and public service organisations is supported by forms of citizen identification and identity management, the management of citizen identity information across government usually involves a patchwork of different and often incompatible approaches, means and systems [22]. Another aspect of more or less unchanged management of citizen identity information in public service relationships is that government has the exclusive right to issue and manage official citizen identification documents, such as the passport or birth certificate, and specific service-related identity information, such as a National Health number or a Social Security Number. Moreover, governments have the exclusive, democratic responsibility to preserve public records, regardless of the format of these records [33].

However, with the introduction of new online public service channels there is an increasing awareness that emerging 'identity issues' in new citizen – government relationships need to be solved. Governments are now entering new digitised public service relationships with individuals, in which they will need to regain confidence on two different levels: the necessity to 'know' the individual with whom they are exchanging public service-related information; and the necessity to ensure that the individual is indeed entitled to receive that information [31]. Citizens too will need to gain trust that the new online public

[2]In some countries, such as New Zealand, permanent residents have more or less similar access to public services compared to citizenship holders.

service environment is authentic, and that the personal information they provide to the public service providing agency is secure and used in accordance with legislative requirements. As a result, around these emerging identity issues in new citizen – government and other online relationships, a new area of scholarly and practitioners' thinking is being developed, also called 'Identity Management' (IDM). Interestingly however, the large majority of scholarly ideas and perspectives that are being developed in this IDM field are narrowly focused on the design and implementation of new digital IDM systems. This implies that the 'legacy' systems, practices, arrangements and procedures of managing citizen identity information in the physical world, including existing citizen – government relationships, usually are not taken into consideration in the development of a citizen IDM perspective or approach. The consequence of this predominantly technical focus on citizen IDM is that comprehensive thinking on the management of citizen identity information in converged digital and physical public service environments, including the wider implications for government, citizens and citizen – government relationships, is hardly available. A good example of this narrow IDM perspective is the widespread assumption that a robust IDM system is a critical enabler for the uptake of e-government services [53]. This assumption however does not take into account the 'robustness' of other non-technical factors influencing the IDM-enabled e-government service relationship with the citizen, such as the citizen's trust in the public service providing agency, the handling of digital citizen identity information by staff members in the back-office of the e-government service relationship, or the sharing of digital citizen identity information across government agencies and other organisations.

Commonly, (digital) IDM is understood and defined as "the set of rules, procedures, and technical components that implement an organisation's policy related to the establishment, use, and exchange of digital identity information for the purpose of accessing services or resources" [10,53]. In general, digital citizen 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 privacy and security of citizen identity information; improved customer convenience and access to public services; and a step increase in the provision of e-government services by enhancing trust and confidence in online interactions with citizens [37,53].A commonly used definition of digital identification is the "association of information items or 'identifiers' with a particular human being" [14]; digital authentication then is defined as "the process of checking an information claim or assertion made by an individual about their identity, ensuring the person is the individual he or she claims to be" [17,25]. Digital identification occurs when an entity compares the identifiers of an individual with a set of identifiers that the entity has previously recorded, and finds a match between the two [27]. Generally, the following categories of digital identifiers are acknowledged [4,20,27]:

- *Something you are* – characteristics that are inherent or attached to an individual's physical body, e.g. DNA, fingerprints, voice or face recognition;
- *Something you do* – characteristics that relate to the behaviour of an individual, e.g. click-behaviour in a digital environment, attitudes in a specific social context;
- *Something you know* – the characteristic of having distinct knowledge, e.g. password, mother's maiden name or another shared secret;
- *Something you have* – the characteristic of possessing a distinct item or 'token', e.g. smart card, an RFID tag attached to your luggage, a software token like a digital certificate;
- *Something you are assigned to* – identifiers that are socially defined for that person, e.g. name, address, title, date of birth, contact phone number, social security number.

These IDM-related definitions and categories of digital identifiers indicate that digital IDM takes place on a different footing compared to paper-based and face-to-face forms of citizen identity management.

Moreover, it becomes clear that the management of citizen identity information is dependent on the public service context and relationship in which an individual shares her personal information with a government agency [38,59]. Consequently, taking into consideration the convergence of digital and physical world-related aspects of managing citizen identity information in emerging public service environments, a broader and deeper understanding of the actual use of new ICT-enabled forms of citizen IDM in citizen – government relationships is needed. In general, the introduction and use of digital IDM in public service relationships with the citizen can potentially lead to the following informational changes [12,37,47]:

- information can flow freely and in ways that are difficult to trace, compared to information in 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 fragmented identity information on the citizen;
- transactions become information dependent;
- 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 informational changes raise a number of new and complex challenges for citizen – government relationships. For example, an important element of robust digital citizen IDM is the security of IDM systems. The OECD [53] observe the following challenges for government in ensuring effective security in digital IDM systems: user confidence of the availability, access, and reliability of digitised personal information; user confidence of the processing and use of digitised personal information by those with legitimate authority and purpose; minimisation of system disruption or corruption; the impact of the technical architecture and design on information security and privacy; auditing of sensitive personal data; and developing processes and procedures to address the possibility of data breaches. *Vice versal* Lusoli et al. [42], point at the emerging challenge of how citizens can be held accountable for the accuracy of their personal information provided in e-government service relationships. A further challenge is to determine ownership of the collected identity information on the citizen, especially in integrated forms of e-government service delivery, and, with that, to establish appropriate rights around access and use of citizen identity information.

Another example is the need for effective public records management and the challenges emerging from existing legislative requirements to apply recordkeeping principles equally to physical and digital public records. Emerging challenges include issues around human fallibility (e.g. storage of typos in public records; accidental deletion of public records); technological fallibility (e.g. system back-up failures); the ease of altering digital records without leaving a trace; the storage of digitised information without metadata; the focus on up-to-date digital data at the expense of historical data; long-term digital storage and technological obsolescence; and the management of public records that only exist or are fully functional within a specific electronic environment, i.e. without a paper equivalent [9,28,33,48].

3. Surveillance State versus Service State perspectives

Considering these informational changes and the complex challenges they generate for the management of citizen identity information, it may not be surprising to observe that scholars point towards fundamental changes happening to citizen – government relationships as a result of the introduction of new digital

forms of citizen IDM [36]. Interestingly however, there seem to be almost opposite views on the direction and outcomes of these fundamental changes [58]. In general, two dominant perspectives are emerging from the literature, which we have described elsewhere as a 'Surveillance State perspective' and a 'Service State perspective' [37]. These competing perspectives are further explained below.

3.1. A Surveillance State perspective

Newly available ICTs, such as CCTV cameras, smart cards, satellites, RFID tags, Internet cookies, email traffic, and mobile phones, offer unprecedented ways to gather and process digitised identity information of individuals. As a result, several scholars take the view that these new digital IDM systems are in fact 'surveillance systems': systems which not only collect and process citizen identity information, but also monitor their behaviour. The outcome of government agencies using these new 'informating' capabilities is that the behaviour of citizens can be influenced on the basis of their identity information. Or, as Murakami-Wood et al. [50] explain: "where we find purposeful, routine, systematic and focused attention paid to personal details ... we are looking at surveillance".

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 [45, p. 2]. For instance, 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, inspection, eligibility, inclusion or exclusion, or access, for example [44,50]. Consequently, surveillance systems are discriminatory technologies as they sieve and "socially sort" for the purpose of assessment, thus affecting people's life chances [44, p. 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 organisations [45, p. 74].

The vast introduction of surveillance systems in our society has led scholars to point at the development of a surveillance society, in which government uses these new digital systems for the collection and processing of citizen identity information, with profound implications for democratic citizen rights (e.g. [43,50,52]). For example, 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 [50]. Another, more recent example is a report on Britain's 'Database State': a survey of 46 central databases across UK government departments, that hold citizen identity information related to many aspects of our lives, such as health, education, welfare, law enforcement and tax. The authors point out that "*many question the consequences of giving increasing numbers of civil servants daily access to our personal information... The emphasis on data capture, form-filling, mechanical assessment and profiling, damages professional responsibility and alienates the citizen from the state. Over two-thirds of the population no longer trust the government with their personal data.*" [3, p. 4]. Although the use of digital IDM systems in citizen – government relationships can support government in its efforts to modernise and rationalise and, with that, to enhance speed, control and coordination in handling individuals' requests to access public services, for example, it is expected that this can bring about substantial information and power imbalances in citizen – government relationships (e.g. [3,41,45,50]).

Alternatively, academics concerned about these developments of surveillance and increased identification of individuals perceive the use of digital citizen IDM systems based on principles of anonymity or pseudonymity as a realistic scenario for government agencies (e.g. academic collaborations in Europe, such as [15,20,24,56]). In their view, government could move away from this Surveillance State perspective and rebalance information relationships with citizens by incorporating privacy into the design

of citizen IDM systems and providing individuals with control over the transmission of their identity information [15,26,54]. Another alternative for government agencies to provide citizens with (more) control over their identity information exchanges with government and, with that, to better protect citizen identity information and enhance citizen trust, would be to increase transparency around the use of citizen identity information [42,51].

3.2. *Service State perspective*

Many scholars point at a strong alignment between opportunities offered by new digital ways of managing citizen identity information and a New Public Management (NPM) style of public service reform, including public service innovation or transformation; customer-focused or personalised public service provision; better coordinated public services; and integrated public service provision (e.g. [2, 6,8,11,21,29,38,39,46,49,58]). In many countries, an increased sharing of citizen identity information has been acknowledged as critically important to cross-government collaboration and the achievement of more efficient and effective public service outcomes [2,7,30,35]. Based on these newly available ICT-facilitated opportunities for managing citizen identity information Dunleavy et al. [18] perceive the opportunity of a response to emerging public sector problems resulting from NPM reforms, with the adoption of a new public management reform model of 'Digital Era Governance'. This Digital Era Governance Model can be characterized under the following three themes [18]:

- 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-focused or needs-based foundation for the organisation of public service provision. Examples are IDM-enabled public service reorganisations around a single-client group or 'ask-once' processes supported by re-using already collected citizen identity information; and
- Digitisation 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 public service applications.

Dunleavy et al. [18] point out that the introduction of new digital citizen 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. This then will lead to improved access to public services, increased effectiveness of public service provision, and, with that, decreasing information asymmetries between the citizen and the State.

These two emerging scholarly perspectives on the Surveillance State and the Service State, respectively, are summarised in Fig. 1.

4. Empirical insights on managing citizen identity in citizen – government relationships

"That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent

Attribute	Surveillance State perspective Meaning	Service State perspective Meaning
Increased and systematic use of digital citizen IDM systems	Surveillance systems leading to rationalization and control	Public service support systems leading to service transformation
IDM objective	Risk management, 'knowing the unknown'; increased efficiency	Targeted public service provision; CRM; increased effectiveness
Purposeful attention to citizen identity information	Surveillance	Better public service provision
Increased information-sharing	Increased analysis, matching and merging of citizen identity information; profiling	Reduced duplication and fragmentation; joined-up government; integrated public service provision
Client focus	Monitoring; segmentation of service users; social sorting	Holistic needs-based service provision; personalization; citizen-centric government
Implications for citizen-government relationships	Increasing information asymmetries; eroding trust	Decreasing information asymmetries; increasing trust
Citizen rights' implications	Violation of privacy and individual freedom rights	Improved access to public services; open government; transparency

Fig. 1. Surveillance state vs. service state perspective. (Source: [37, p. 843]).

of such protection" [62]. In their seminal article Warren & Brandeis [62] make a case for the introduction of a right to privacy under existing legislation, due to the invasion of the individual's private life caused by new and profound technologies at the time, namely instantaneous photographs and newspapers. Since then, the necessity to regularly redefine the exact nature and extent of an individual's privacy protection as a result of the introduction of new technologies in our society has not at all diminished in importance [9, 51]. Other new technologies, such as digital citizen IDM systems, have been introduced in public service relationships with citizens, with, if we consider the two scholarly perspectives described above, a likely fundamental impact and implications for citizen – government relationships.

So far however, these two perspectives of the Surveillance State on the one hand and the Service State on the other, are largely sustained by *a priori* reasoning about ICT-enabled informational changes rather than by a clear empirically derived evidence base that casts light upon what is actually happening with citizen identity information in emerging e-government service environments [37]. In general, there is not much empirical in-depth knowledge available on the management of citizen identity information in these new digital public service relations between citizens and government, and the implications, including those in the area of privacy [51]. The knowledge on changing informational relationships we do have, usually is collected via quantitative surveys which, subjectively and with a certain bias, tend to inquire about the 'concerns' people have with regard to their privacy protection in a society that is changing as a result of the introduction of new ICTs [9,51]. However, available empirical studies suggest a significant discrepancy between individuals' expressed concerns about their privacy and their actual behaviour in online environments [61,23,51].

This empirical observation further raises the demand for empirical research into emerging ICT-enabled citizen – government relationships. In this contribution, empirical insights from three substantial research

projects are introduced as stated in section 1 of this paper. Together, these three research activities provide empirical insights from both sides of public service relationships: from the perspective of government on the one hand, and from a citizen perspective on the other. Although empirical data have been collected in different countries and public service contexts, which sets limits towards generalisation of the findings, these research findings can at least help us to identify and unpack to some extent the nature, direction and implications of these emerging ICT-supported citizen-government relationships.

4.1. Empirical insights from a government perspective

In a UK-based empirical research project 'Personal identification and identity management in new modes of e-Government' [40], the actual use of citizen IDM systems by government agencies in eight case studies of e-Government service relationships with citizens were explored. The findings from this research show that no particular perspective is dominant, but that attributes of both a Surveillance State perspective and a Service State perspective are observable simultaneously and in parallel in these case studies, albeit within the legal restrictions of UK data protection legislation and not violating a citizen's privacy rights therefore [58,37].

A multifunctional smart card application used by a UK local government to provide individuals with various public services, including library services, public transport, leisure facilities' access, and services at secondary schools, provides a first example. The card makes use of the identity information for promoting 'good citizen behaviour': for instance, a citizen can accrue loyalty points by choosing healthy food options in the school canteen, or from class attendance data, or for using environmentally friendly bins for rubbish collection. These loyalty points can be exchanged against products and services offered by local retailers. The smart card is available on a voluntary basis and free-of-charge to those who live, work or visit the borough. In accordance with UK data protection legislation, smartcard-supported access to public service environments is enabled on the basis of an individual's consent, and there is no sharing of citizen identity information across public service domains or providers. Furthermore, senior citizens entitled to concessionary travel service on local buses and pupils entitled to free school meals do not need to load money on their card but can use it as a service entitlement card by presenting the card to the official concerned in the same way as anybody else. Consequently, in this case study, we can observe both Surveillance State attributes, such as monitoring, segmentation of service users, merging of citizen identity information, and increased analysis, and Service State attributes, such as customer relationship management, targeted public service provision, and improved access to public services.

Two further case examples in which both Surveillance State and Service State attributes can be observed, are the use of Automatic Number Plate Recognition (ANPR) cameras in policing services and an online provisional driver's licence application service accessible through the UK Central Government's Direct.gov web portal. In the ANPR case study, number plate information collected with ANPR cameras mounted in police cars, is matched against a large number of datasets from a variety of public and private sector databases in an attempt to detect and reduce crimes and misdemeanours. Once a few hits occur across the multiple databases, police officers make a professional judgement to pursue the vehicle. The use of ANPR cameras in policing services has led to an increased effectiveness in public service provision, with a fivefold increase in the arrest rate for the police force under study, and more equitable public service provision as a result of using ICT-mediated empirical evidence instead of postulations which may be a consequence of human prejudice (e.g. race, social class).

In the case of the online provisional driver's licence application service, the applicant's digital identity information not only is matched with the database of the responsible government agency to explore

eligibility on the basis of potential previous applications and driving disqualification information, but also is transferred to a private sector information solutions provider to assess the applicant's 'digital footprint' across a number of public and private databases (e.g. banking databases, mail-order catalogue databases), seeking assurance that the identity data are bona fide and generating a 'trust' score which determines whether the application can be completed online. If the applicant fails the digital footprint assessment, he or she will be instructed to complete the process via a face-to-face service channel.

These three case study examples not only demonstrate that citizen identity information has become a critical element of new digital public service relationships, with public servants becoming increasingly reliant upon digitised citizen identity information for service-related assessments and decision-making instead of paper-based or face-to-face interaction for example, but also that citizen identification and the management of citizen identity information no longer is an exclusive area for a single government agency or even the public sector at large. Private sector organisations have become important actors in this space, ranging from involvement in citizen authentication and the assessment of public service access on the basis of digital footprints across public and private sector databases, to the management of citizen IDM infrastructure and citizen identity information stored in public sector databases. Moreover, research findings of two other case studies from this same research project, namely the electronic monitoring of youth offenders detained in their home environment and the use of mobile communications to provide critical health services to individuals in the back of an ambulance, show that citizen IDM technologies to a certain extent can replace human interaction in the service delivery chain.

Furthermore, research findings from the emergency services case study and a case study on the use of a call centre for providing national health services to individuals demonstrate that public servants do not always need to know generic citizen identity information, such as name, address, or date of birth, to provide services to citizens. In these two case studies, only minimal personal information, such as characteristics related to personal health, are needed to establish a service. This situation corresponds with the scholarly response to Surveillance State-type developments in having privacy values 'designed into' the management of citizen identity information.

These research findings of supporting a privacy-friendly approach to the sharing of citizen identity information in public service provision resonate with a New Zealand-based research project 'Improving Information sharing for effective social outcomes' [35]. In this research project, eight case studies of cross-agency information sharing practice focused at providing ICT-supported integrated public services to individuals with multiple complex needs, such as the unemployed, refugees, or prolific offenders, were empirically explored. The findings from this study show that professionals share information related to individual clients with colleagues from other organisations on a 'need to know' basis to ensure that colleagues know enough to do their jobs effectively and safely. Commonly, abstracted information is used to alert other professionals about the need to investigate a particular client. In general, professionals are conscious about the need to protect citizen identity information but apply 'common sense' in cases where that protection of an individual's personal information might stand in the way of the protection of professional, personal, or community safety. Consequently, although there are situations in which professionals breach the privacy legislation on the basis of public safety considerations, from a citizen rights' perspective the sharing of citizen identity information under those circumstances is actually to the advantage of the individual. Or, as a research participant pointed out: *"if I break the law I do it for the right reasons"*.

Moreover, in accordance with New Zealand privacy legislation, all case study organisations have clear, documented processes whereby individuals consent to particular sets of their identity information being shared with other professionals and across public sector agencies. However, the consent forms

used across the initiatives under study vary in detail and depth. For example, in a case study looking at electronically monitored bail of individuals awaiting their trial in court, applicants to this EMBail initiative need to sign a consent form that enable New Zealand police assessors access to a wide range of citizen identity information related to the individual's offending history, family and daily living circumstances, and social service needs, and to share that identity information with other officials from various agencies. In this particular case, a citizen who wants to participate in this initiative only can do so by signing away her right to privacy protection.

Furthermore, the research findings show that, across the various cross-agency collaborative initiatives, each agency has its own information storing processes including secured databases containing citizen identity information pertinent to their own mandate and with information access restricted to agency personnel only. This not only leads to a situation in which each agency has fragmented identity information on an individual, but also that officials use manual 'work-around' techniques to compensate for this restricted access regime or the lack of interoperability between information systems belonging to different agencies. These manual 'work-around' techniques involve the duplication of citizen identity information, the duplication of data entry processes, and the distribution of emails with sensitive citizen identity information in attachments across the agencies involved. Consequently, although the privacy rights of individuals may be protected by an IDM approach of agency-based databases and restricted access to those databases, it is clear that the security of citizen identity information is at risk in these cases. For instance, human errors in (duplicated) data entry processes or the relatively easy access of unauthorised people to email attachments with citizen identity information may have fundamental implications for citizen – government relationships.

4.2. Empirical insights from a citizen perspective

In a recently completed New Zealand-based research project 'Public attitudes to the sharing of personal information in the course of online public service provision' [32], the attitudes of 63 members of the general public towards the disclosure, collection, management, and sharing of citizen identity information in the front-office and, to a certain integrated extent, back-offices of public bodies were explored in ten intensive focus group meetings. The research findings show that the majority of participants have a benign view of the sharing of citizen identity information with and across the New Zealand public sector. Generally, the participants in this study have a high trust in the New Zealand government and its agencies, and believe that they are working in the best interests of citizens. Exceptions however could be found among participants with a high dependency on social services; Māori[3]; Pasifika[4]; and self-employed participants.

These exceptions show that context and culture are determining factors for peoples' attitudes towards the sharing of identity information with and across government agencies. For instance, high service dependent participants and those who are self-employed perceive all identity information as private information, and only want to share identity information with government reluctantly and if they have to, as government agencies "are not working for them". Furthermore, high service dependent participants see clear negative power imbalances and information asymmetries between themselves and public sector agencies. These negative feelings of distrust and powerlessness towards public sector agencies were also present among Māori and Pasifika participants with some subtle differences: for instance, whereas

[3]Indigenous people of New Zealand
[4]People from the Pacific islands

Māori particularly are negative about the integrity and Māori language use of individual public service staff members, Pasifika people find dealing with government agencies difficult and feel demeaned by the process.

In general, the research population turned out to be 'privacy pragmatists' (cf. [1]): individuals who are prepared to disclose their identity information to government agencies in return for enhancements of public service provision or other personal or collective benefits. However, the research participants were not indifferent about their privacy, and clearly pointed at the need for public service agencies "to play privacy by the rules" by using collected identity information only for the intended purpose and asking clients for consent.

Moreover, transparency about the use of citizen identity information by government agencies was generally absent amongst the research participants. Participants provide their identity information to public sector agencies in order to obtain the service, but they usually do not understand how their identity information will be processed or used; why they need to fill in multiple forms with the same identity information; how and to what length their identity information will be stored or kept; and who will have access to their identity information, for example. Furthermore, participants showed limited knowledge about the sharing, or non-sharing, of identity information between government agencies and with other organisations. An area of concern to a number of research participants was the accuracy of identity information stored and processed by government agencies, and particularly identity information used for categorising clients and determining eligibility for services. Several research participants noted problems with incompetent frontline staff members making mistakes with the handling and processing of citizen identity information. This lack of transparency and perceived administrative incompetence made participants feel uncomfortable about the sharing of identity information with and across government, and wanting to have more control over the identity information they provide to public sector agencies. This particular response was stronger among those participants who are more distrustful of government agencies, such as high service dependent, Pasifika, Māori, and self-employed participants.

A tension in participants' perspectives could be observed in discussing the advantages and disadvantages of cross-agency information sharing at a collective level of interest, and at a personal level of interest. From a collective interest point of view, the majority of participants saw clear benefits of cross-agency information sharing, such as increased effectiveness in public service provision to individuals and a fair allocation of taxpayer funded services, and were permissive therefore. Several participants also pointed at advantages of cross-agency information sharing at a personal level, such as simple and convenient public services, fair public service provision for those who play the game in accordance with the rules, and efficient public service provision. However, where participants perceived disadvantages of cross-agency information sharing at a personal level of interest, they tended to be more protective of their identity information and pointed at the requirement for privacy protection. For instance, vulnerable individuals, particularly those highly dependent on social services, tended to regard identity information that could be used against them, or identity information that might lead to a misjudgement in public service provision, as private information. Other high users of social services, such as senior citizens, believed that they are asked too much private information and felt they do not have any choice about providing the requested identity information as they need the service. Furthermore, participants generally felt uncomfortable in disclosing identity information to government agencies with an eligibility monitoring function and/or powers to force compliance.

Several participants were concerned that frontline staff members are not asking for the relevant identity information in order to provide the right service to them. Furthermore, participants expressed difficulties in finding and joining up the bits of public service information that are relevant to them. Research

Attribute	Fair State Perspective Meaning
Increased and systematic use of digital citizen IDM systems	Efficiency support systems leading to value for the taxpayer's money and treating citizens fairly
IDM objective	Increased processing and rationing of public service clients; increased efficiency and equitable enforcement
Purposeful attention to citizen identity information	Fairness in public service use
Increased information sharing	Improved decision-making by individual public service providing agencies; Improved compliance; Increased efficiency for citizens in their role as taxpayer and public service customer
Client focus	Improved administration; fair and equitable public service provision; organisation-centric government
Implications for citizen-government relationships	Information asymmetries in citizen-government relationships are clear and applicable to all;
Citizen rights' implications	Equality under the Law

Fig. 2. Fair State perspective. (Source: [32, p. 102]).

participants experienced limitations of standardised form filling and a lack of relevant and integrated public service information in accessing public services online. For some, the lack of provision for adding relevant identity information to their specific case in an online form is the reason they prefer to speak to a staff member, rather than using the e-channel for public service consumption.

Most of the research participants showed that they valued attributes belonging to a Service State perspective in their attitudes towards cross-agency information sharing, such as better public service provision and increased service effectiveness; only some of them showed concerns associated with a Surveillance State perspective, such as increased information asymmetries, eroded trust, social sorting and "putting people in the wrong [bureaucratic] box". Although research participants generally supported cross-agency information sharing for the achievement of a Service State perspective, they did not see specific attributes of a Service State perspective, such as reduced duplication, holistic needs-based service provision and improved access to public services, in the public service relationships they have experienced thus far. Instead, research participants referred to attributes which neither belong to a Service State perspective nor a Surveillance State perspective. The attributes they put forward seem to constitute an alternative scenario of a Fair State perspective: a perspective of government using new ICT-enabled forms of citizen IDM to deliver fair and efficient modernised public services to its citizens in

an equal way, in accordance with collectively determined rules and interests. More specifically, attributes emerging under this Fair State perspective are more efficient public management systems and value for money for the taxpayer; more efficient and equitable enforcement; more fairness in public service use; improved decision making by government agencies; improved administration and management of public records; reduction in information asymmetries; and equality under the Law. A summary of this Fair State perspective is provided in Fig. 2.

5. Rethinking citizen – government relationships in the digital age

Citizen identity information has become a critical element of ICT-enabled public service relationships between governments and citizens. The empirical insights provided above show that, not only have public servants become reliant upon digital citizen identity information for public service-related assessments and decision-making, but also citizens are aware of the strong 'currency' of their identity information in reciprocal public service relationships across varying public service environments. Moreover, as a result of the use of digital citizen identity information in public service environments, citizen – government relationships are changing profoundly and in varied ways: for example, digital citizen identity information is used by governments to support those citizens who are 'loyal' to the collective interests of the State by rewarding good citizen behaviour; to distribute public service entitlements in a more equitable, anonymous way; to strongly increase public service effectiveness and make unprejudiced, evidence-based public service assessments; and to generate trust scores on citizens to determine who is trustworthy enough to be offered full access to e-government services.

Consequently, the fundamental changes in citizen – government relationships that are happening as a result of the use of digital IDM systems in public service provision have different directions and therefore lead to varying outcomes: both increasing and decreasing information asymmetries between the State and the citizen are observable, even in cases where the same citizen IDM technology is used by government within a particular public service context. Similarly, from a citizen perspective, power balance perceptions related to the management of citizen identity information in public service provision can be fundamentally different for various groups of citizens. Moreover, there is no clear perspective on the role of the State in the use of digital citizen IDM emerging from the research findings: attributes of the three perspectives identified in this contribution, namely the Surveillance State, Service State and Fair State perspectives, can be observed simultaneously and in parallel across the three empirical research projects. For example, in some case study examples, by allowing the Surveillance State to operate Service State-type and/or Fair State-type outcomes can be achieved, such as increased effectiveness in public service provision, improved access to public services, and more evidence-based and equitable public service provision. Another example derives from the different Fair State and Surveillance State perspectives on cross-agency information sharing where vulnerable citizens simultaneously have both a collective level of interest and a personal level of interest, respectively. These research findings demonstrate the importance of considering the specific public service context and public service relationship with the citizen as determining factors in developing attitudes towards and perspectives on digital citizen IDM in emerging public service environments.

At the same time however, the management of digital citizen identity information no longer is the exclusive responsibility of the State. Although largely hidden to members of the general public, private sector organisations have become important players in the management of digital citizen IDM. This observation raises important accountability and transparency issues, including issues regarding access to citizen identity information.

Furthermore, the research findings show that informational changes in citizen – government relationships are, with some exceptions, in accordance with data protection legislation. From a citizen perspective, although the general expectation is for government to 'play privacy by the rules', citizens are in fact willing to disclose (more) identity information to government in return for better public service provision or other benefits. From a government perspective, it is interesting to observe that in some public service environments, such as health and emergency services, there is awareness that only minimal citizen identity information is needed in order to provide services, leading to default 'privacy by design' management of citizen identity information. In those situations where professionals breach data protection legislation, the individual customer can in fact be better off. However, an important issue emerges in situations where public service provision is happening in accordance with the legislation, but citizens are forced to disclose (a wide range of) their identity information if they want to access that particular service.

Other fundamental issues emerging from using digital citizen IDM in citizen – government relationships are the security and accuracy of the identity information government holds on the citizen, especially the risks caused by human errors or interventions. These information security and accuracy risks can have fundamental implications for power balances between the State and the citizen and, with that, for citizen rights and citizenship-related public service entitlements. To citizens, also a reverse identity information issue can be an important part of information asymmetries in new ICT-enabled public service relationships, for instance when officials do not ask the citizen for the relevant identity information in order to provide the right service to that particular individual.

Generally, in the age of digital citizen identity, information, the 'social contract' between the citizen and the State is becoming more and more fluid, with fundamental changes happening in citizen – government relationships. From different perspectives – perspectives from scholars, government, and citizens, for example -, the direction and implications of these changes vary substantially however, thus demanding for more empirical research within varying public service contexts. Moreover, the informational changes happening to citizen – government relationships as a result of using digital citizen IDM are largely hidden, unknown or ambiguous to members of the general public. Consequently, in order to see these changes and explore the issues and implications in a public debate for instance a comprehensive view, rather than a narrow technical one, on the management of digital citizen identity information in public service environments is an important requirement. Furthermore, governments will need to offer more transparency about the management and use of digital citizen identity information if they want their citizens to support a Fair State or Service State perspective on fundamental informational changes in citizen – government relationships.

References

[1] P. 6, K. Lasky and A. Fletcher, *The future of privacy*, Vol. 2: Public Trust and the use of private information, London: Demos, 1998.

[2] P. 6, C. Raab and C. Bellamy, Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part 1, *Public Administration* 83(1) (2005), 111–133.

[3] R. Anderson, I. Brown, T. Dowty, P. Inglesant, W. Heath and A. Sasse, *Database state*, York: The Joseph Rowntree Reform Trust Ltd, 2009.

[4] B. Anrig, E. Benoist and D.O. Jaquet-Chiffellet, Virtual Identity, paper delivered within the scope of the European project Future of Identity in the Information Society (FIDIS) available at http://www.vip.ch/papers/virtual_identity.pdf, 2004.

[5] J. Backhouse and R. Halperin, A Survey on EU Citizen's Trust in ID systems and authorities, *Identity in the Information Society* (2007).

[6] V.J.J.M. Bekkers and V. Homburg, E-Government and NPM: A Perfect Marriage? in: *The information ecology of E-Government*, V.J.J.M. Bekkers and V. Homburg, eds, Amsterdam: IOS Press, 2005.

[7] C. Bellamy, C. Raab, A. Warren and C. Heeney, Institutional shaping of interagency working: Managing tensions between collaborative working and client confidentiality, *Journal of Public Administration Research and Theory* **17**(3) (2007), 405–435.
[8] C. Bellamy and J.A. Taylor, *Governing in the Information Age*, Buckingham: Open University Press, 1998.
[9] C. J. Bennett and C. Raab, *The governance of privacy: Policy instruments in global perspective*, Aldershot, UK: Ashgate, 2003.
[10] D.G.W. Birch, *Digital Identity Management, Perspectives on the technological, business and social implications*, Aldershot: Gower Publishing Limited, 2007.
[11] S. Borins, K. Kernaghan, D. Brown, N. Bontis, P. 6 and F. Thompson, (eds), *Digital State at the Leading Edge*, Toronto: University of Toronto Press, 2007.
[12] J. Camp, *Identity in Digital Government: A Research Report of the Digital Government Civic Scenario Workshop*, Cambridge: Kennedy School of Government, 2003.
[13] J. Caplan and J. Torpey, (eds), *Documenting Individual identity: the development of state practices in the modern world.* Princeton, NJ: Princeton University Press, 2001.
[14] R. Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues, *Information Technology and People* 7(4) (1994), 6–37.
[15] R. Clarke, Introduction to dataveillance and information privacy, and definitions of terms. Retrieved from http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html, 1997.
[16] R. Clarke, Dissidentity, identity in the information society. Retrieved from http://www.springerlink.com/content/2738929u634861073/fulltext.htm, 2009.
[17] M. Crompton, Proof of ID required? *Getting Identity Management Right, Paper Presented at the Australian IT Security Forum*, Sydney: Office of the Federal Privacy Commissioner, 2004.
[18] P. Dunleavy, H. Margetts, S. Bastow and J. Tinkler, *Digital Era Governance: IT Coporations, the State, and E-Government*, Oxford: Oxford University Press, 2006.
[19] K. Faulks, *Citizenship*, London: Routledge, 2000.
[20] FIDIS, Future of identity in the informaiton society: Identity in a networked world – use cases and scenarios. Retrieved from http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.6_Ident ity_in_a_Networked_World.pdf, 2006.
[21] J. Filipe Araujo, Improving Public Service Delivery: The Crossroads between NPM and Traditonall Bureaucracy, *Public Administration* (2001), 915–932.
[22] J. Fishenden, *eID: Identity Management in an Online World*, paper presented at the 5th European Conference on e-Government, Antwerpen, Belgium, 2005.
[23] S. Fox, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, Research paper, Washington: Pew Research Center, 2000.
[24] D. Gilbert, I.R. Kerr and J. McGill, The medium and the message: Personal privacy and the forced marriage of police and telecommunications providers, *Criminal Law Quarterly* **51**(4) (2006), 469.
[25] D. Greenwood, *The Context for Identity Management Architectures and Trust Models*, paper presented at the OECD Workshop on Digital Identity Management, Trondheim, 2007.
[26] M. Hansen, P. Berlich, J. Camenish, S. Clauss, A. Pfitzmann and M. Waidner, Privacy-enhancing identity managment, *Information Security Technical Report* **9**(1) (2004), 35–44.
[27] J. Harper, *Identity Crisis, How Identification is Overused and Misunderstood*, Washington D.C: the Cato Institute, 2006.
[28] M. Hedstrom, Electronic recordkeeping, *Encyclopedia of Library and Information Science* (2000), 160–169.
[29] C. Hood, A Public Management for all Seasons? *Public Administration* **69** (1991), 3–19.
[30] K. Kernaghan, Beyond Bubble Gum and Goodwill: Integrating Service Delivery', in: *Digital State at the Leading Edge*, S. Borins, K. Kernaghan, D. Brown, N. Bontis, P. 6 and F.Thompson, eds, Toronto: University of Toronto Press, 2007, pp. 102–136.
[31] A.M.B. Lips, E-Government under construction: challenging traditional conceptions of citizenship, in: *E-Government in Europe. Rebooting the state*, P. Nixon and V. Koutrakou, eds, Routledge, London, 2007, pp. 33–47.
[32] A.M.B. Lips, E. Eppel, A. Cunningham and V. Hopkins-Burns, Public attitudes to the sharing of personal information in the course of online public service provision, Final Research Report. Wellington: Victoria University of Wellington. This research project was financially sponsored by the New Zealand Inland Revenue Department, Victoria University of Wellington, Datacom Systems Ltd, State Services Commission, Department of Internal Affairs, FX Networks Ltd, and Microsoft New Zealand, 2010.
[33] A.M.B. Lips and A. Rapson, *Exploring Public Recordkeeping behaviors in Wiki-Supported Public Consultation Activities in the New Zealand Public Sector*, Paper presented at the 43rd Hawaii International Conference on System Sciences (HICSS-43), Hawaii, 2010.
[34] A.M.B. Lips, J.A. Taylor and J. Organ, Identity management in e-Government service provision: Towards New Modes of Government and Citizenship, in: *Understanding E-Government in Europe: Issues and challenges*, P.G. Nixon, V.N. Koutrakou and R. Rawal, eds, London: routledge, 2010, pp. 151–168.

[35] A.M.B. Lips, R.R. O'Neill and E.A. Eppel, Improving information sharing for effective social outcomes, Emerging Issues Programme Research project Report, Wellington: Victoria University of Wellington, December 2009.
[36] A.M.B. Lips, J.A. Taylor and J. Organ, Identity management, administrative aorting and citizenship in new modes of government, *Information, Communication and Society* **12**(5) (2009), 715–734.
[37] A.M.B. Lips, J.A. Taylor and J. Organ, Managing citizen identity information in e-government service relationships in the UK: The ememrgence of a surveillance state or a service state? *Public Management Review* 11(6) (2009), 833–856.
[38] A.M.B. Lips, J.A. Taylor and J. Organ, Identity Management as Public Innovation: Looking Beyond ID Cards and Authentication Systems, in: *ICT and Public Innovation: assessing the modernisation of public administration*, V.J.J.M. Bekkers, H.P.M. van Duivenboden and M. Thaens, eds, Amsterdam: IOS Press, 2006.
[39] A.M.B. Lips, S. Van der Hof, J.E.J. Prins and A.A.P. Schudelaro, *Issues of Online Personalisation in Commercial and Public Services Delivery*, Nijmegen: Wolf Legal Publishers, 2006.
[40] A.M.B. Lips, J.A. Taylor and J. Organ, *Personal identification and Identity Management in New Modes of E-Government*, Economic and Social Research Council e-Society Project, Ref: RES-341-25-0028, 2005–2007.
[41] London School of Economics, The Identity Project. An assessment of the UK Identity Cards Bill and its implications): The LSE Identity Project Final Report, June 2005.
[42] W. Lusoli, I. Maghiros and M. Bacigalupo, eID policy in a turbulent environment: Is there a need for a new regulatory framework? *Identity in the Information Society*, 2009.
[43] D. Lyon, (ed.), *Theorizing Surveillance: The Panopticon and Beyond*, Cullompton: Willan Publishing, 2006.
[44] D. Lyon, Surveillance as social sorting. Computer codes and mobile bodies, in: *Surveillance and Social Sorting: privacy, risk and digital discrimination*, D. Lyon, ed., London: Routledge, 2003, pp. 13–30.
[45] D. Lyon, *Surveillance Society. Monitoring everyday life*, Buckingham: Open University Press, 2001.
[46] H. Margetts, Electronic Government: A Revolution in Public Administration? in: *Handbook of Public Administration*, B.G. Peters and J. Pierre, eds, London: Sage, 2003, pp. 366–376.
[47] G.T. Marx, What's New About the New Surveillance? Classifying for Change and Continuity, *Knowledge, Technology, and Policy* **17**(1) (2004), 18–37.
[48] A. Meijer, Transparent government: parliamentary and legal accountability in an information age, *Information Polity* **8** (2003), 67–78.
[49] I. McLoughlin, G. Maniatopoulos, R. Wilson and M. Martin, Hope to die before you get old? Techno-centric versus user-centred approaches in developing virtual services for older people, *Public Management Review* **11**(6) (2009), 857–880.
[50] D. Murakami-Wood, K. Ball, D. Lyon, C. Norris and C.D. Raab, A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network. The Full Report is available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf, 2006.
[51] H. Nissenbaum, *Privacy In Context: Technology, Policy and the Integrity of Social Life*. California: Stanford University Press, 2010.
[52] T. Ogura, Electronic Government and Surveillance-Oriented Society, in: *Theorizing Surveillance: The Panopticon and Beyond*, D. Lyon, ed., Cullompton: Willan Publishing, 2006.
[53] Organisation for Economic Co-operation and Development, *The role of digital identity management in the internet economy: A primer for policy makers*, Directorate for Science Technology and Industry, Paris: OECD, 2009.
[54] A. Pfitzmann and M. Hansen, *Anonymity, unlinkability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology (v0.3 ed.)*, 2006.
[55] C. Pollitt, Bureaucracies remember, post-bureaucratic organizations forget? *Public Administration* **87**(2) (2009), 198–218.
[56] PrimeLife, PrimeLife – Bringing sustainable privacy and identity management to future networks and services, a research project sponsored by the European Commission, further information can be found at http://www.primelife.eu/, 2008–2010.
[57] I. Th. M. Snellen, Street level bureaucracy in an informaiton age, in: *Public administration in an information age*, I. Th. M. Snellen and W. van de Donk, eds, Amsterdam: IOS Press, 1998, pp. 497–505.
[58] J. A. Taylor, A. M. B. Lips and J. Organ, Idenfitication Practices in Government: Citizen Suveillance and the Quest for Public Service Improvement, *Identity in the Information Society* 24 February 2009, *available at: http://www.springerlinker.com/content/2p127317127324 52.*
[59] J.A. Taylor, A.M.B. Lips and J. Organ, Information-Intensive Government and the Layering and Sorting of Citizenship, *Public Money and Management* **27**(2) (2007), 161–164.
[60] J. Torpey, *The invention of the passport: surveillance, citizenship and the state*. Cambridge: Cambridge University Press, 2000.
[61] A. Viseu, A. Clement and J. Aspinall, Situating privacy online: Complex perceptions and everyday practices, *Information, Communication and Society* 7(1) (2004), 92–114.
[62] S.D. Warren and L.D. Brandeis, The Right to Privacy, *Harvard Law Review* **4** (1890), 193–220.