European Journal of Information Systems (2014) 23, 17–35

www.palgrave-journals.com/ejis/

EDITORIAL

Who do you think you are? A review of the complex interplay between information systems, identification and identity

Edgar A. Whitley[1], Uri Gal[2] and Annemette Kjaergaard[3]

[1]Department of Management, London School of Economics and Political Science, U.K.; [2]University of Sydney Business School, University of Sydney, Australia; [3]Department of Intercultural Communication and Management, Copenhagen Business School, Denmark.

Correspondence: Edgar A. Whitley, Information Systems and Innovation Group, Department of Management, London School of Economics and Political Science, Houghton Street, London WC2A 2AE, U.K.
E-mail: E.A.Whitley@lse.ac.uk

Abstract
This paper introduces the special issue on information systems, identity and identification. In addition to introducing the papers in the special issue, it provides a state-of-the-art review of research into identity and identification to contextualise the contributions of the special issue papers. The paper reviews research themes in personal and organisational identity as well as research challenges in identification before considering the interplay between these two strands.
European Journal of Information Systems (2014) **23,** 17–35. doi:10.1057/ejis.2013.34

Keywords: social identity; organisational identity; identification; biometrics; privacy; security

Introduction

Answers to the questions 'Who am I?', 'Who are we?' and 'How do others know who I am?' reveal the complexity of a topic (more accurately series of topics) that have become increasingly popular in recent years. Scholars from different organisational and management fields, including information systems, have answered the question in a wide variety of ways. From one perspective, the answer to the question can be found in various forms of technological *identification* mechanisms (*credentials*) such as usernames, smart cards and official documents like passports. These mechanisms seek to provide a level of assurance to others as to claims made by the individual – my state-issued passport can be used to provide others with assurance as to my name and nationality whereas my username links me to my account with an online service provider. Where individuals can choose which mechanisms they use to identify themselves, questions of functionality, ease of use and cost come to be important.

From another perspective, technology is transforming the way individuals, groups and organisations think about and define their *identity*. Some individuals may define themselves as mobile workers whose smartphones enable more flexible work patterns than were possible previously. Other individuals may use social media to experiment with aspects of their identity online and act in ways that are not possible in the physical world. Groups may reshape their understanding of who they are as a professional group if the use of a specific technology forces them to spend time on tasks that they find less important; for example if they need to do more administrative work instead of spending time on what they perceive as professional tasks. Organisations, too, can use social media to project a certain collective identity or several dominating identities to external as well as internal

stakeholders. For example, effective use of social media can help transform external perceptions of the enterprise, making it appear much more responsive and customer facing. In addition, technology-enabled capabilities may reconfigure an organisation's operations and relationships with external stakeholders and reshape how it sees itself in relation to them.

Academically, the analytical separation between what Lyon (2009) describes as the technological issues of *identification* and the social issues of organisational and personal *identity* is proving to be arbitrary and increasingly unhelpful for studying contemporary practice. For example, a person's identity as performed through a social networking profile, such as a twitter handle, might end up also being the log – in identification for a series of unrelated online sites. Similarly, online identification mechanisms may inform the way individuals, or groups within an organisation, are perceived by their co-workers and hence shape their identities as organisational members.

It was precisely to explore this complex interplay between information systems, identification and identity that this special issue was organised. The special issue solicited original research in information systems that studied questions of identity/identification. This issue contains four exemplary papers that examine the role of information systems in the complex interplay between identification and identity. Information about the papers, as well as the review process that was adopted for the special issue, is given below. However, in order to contextualise the contributions that the research presented in this issue make, it is helpful to begin by reviewing the current state of research in this space. To simplify things, this review initially separates out research relating to personal, social and organisational identity from research around questions of identification. However, in keeping with the spirit of the special issue call, the review ends by explicitly addressing the interplay between technical issues of identification and social issues of identity. The review also highlights areas where information systems researchers can make useful contributions to our understanding of identity and identification.

Researching identity

Research of identity in an organisational context has become increasingly popular in recent years (Albert *et al*, 2000; Gioia *et al*, 2000; Haslam & Ellemers, 2005; Corley *et al*, 2006; Cornelissen *et al*, 2007). The interest in identity is diverse, reflecting perspectives that originate in the fields of organisation studies, corporate communications, social and organisational psychology, personnel and human resources and strategy and marketing (Cornelissen *et al*, 2007). Furthermore, theoretical and empirical research has explored identity processes as well as their organisational outcomes at various analytical levels from personal to social to organisational (Cornelissen *et al*, 2007).

The growing interest in identity issues reflects the concept's centrality to the way scholars from different disciplines understand and theorise about organisations and about the way people act and interact within them. In addition, it underscores the importance and practical relevance of the concept to a variety of organisational areas including strategy (Dutton, 1997), management and leadership (Gioia & Chittipeddi, 1991; Pratt & Foreman, 2000), inter-organisational collaboration (Beech & Huxham, 2004) and corporate communication (Schultz *et al*, 2000; Cheney & Christensen, 2001).

Despite the broad applicability and use of the concept in general management and organisational studies, it has only been sporadically used in information systems research (e.g., Walsham, 1998; Barrett & Walsham, 1999; Lamb & Davidson, 2005). This is surprising given the significance of identity to a variety of issues that have received considerable attention from information systems researchers such as group and organisational sense-making (Weick, 1995), the shaping of organisational practices and change (Gioia *et al*, 2000; Corley & Gioia, 2004), organisational learning (Corley & Gioia, 2003) and knowledge work (Nag *et al*, 2007).

Although identity research in management studies does not focus on technology in general or information systems in particular, focusing on identity issues in organisations has the potential to help scholars to produce thoughtful and meaningful insights into individual and collective self-constructions in organisations and into the interactions between the implementation and use of information and communications technologies, organisational processes and people.

To explore this potential the next section presents the concept of identity, in particular with respect to its application in organisational settings.

The concept of identity in organisations

The increase in theoretical and empirical identity research in organisational settings can be attributed to the richness of the concept and the opportunity that it provides to explore a wealth of issues that are of interest to scholars from multiple fields. In the organisational domain, this research spans several levels of analysis, ranging from individual (or personal), to social, to organisational.

Personal identity typically refers to unique individual characteristics that are assumed not to be shared with other people and which do not indicate or derive from group membership (Alvesson *et al*, 2008). These characteristics do not equate, in our view, to what is conventionally referred to as personality in the psychology literature. For instance, Jung postulated that personality traits capture individual differences in terms of their preferences for acquiring and processing information (Jahng *et al*, 2002) and can be described along four dimensions: extroversion–introversion, sensation–intuition, thinking–feeling and judgmental–perceptual (Jung, 1971). However, while personality types are cognitively-based and assumed to

be consistent across contexts, we conceptualise personal identity as practice-based, relational and therefore dynamic (Weick, 1995).

Different from personal identity, social identity refers to an individual's perception of him or herself, resulting from his or her membership in a social group (Tajfel & Turner, 1979). Moving up the analytical scale, organisational identity is generally understood to be the collective understanding of members of an organisation of the features that are presumed to be central, distinctive and relatively permanent about the organisation (Albert & Whetten, 1985; Dutton *et al*, 1994).

Common to most theoretical and empirical accounts of organisational identity is the view that identity is rooted in a deep cultural level of the organisation (Gioia *et al*, 2000), residing in interpretive schemes that organisational members collectively construct to provide meaning to their shared history, experiences and activities (Gioia, 1998; Ravasi & Schultz, 2006).

Despite the apparent distinctions separating the different levels of analysis, several scholars have emphasised their similarities and called for a more holistic understanding of identities in organisational contexts. For example, Alvesson *et al* (2008) maintained that 'despite the appeal of persistent distinctions between personal and social identities … we also wish to resist the often arbitrary clarity of such divisions. Instead … we develop a sharper eye for the diverse and fine-tuned ways in which the personal–social relation might be configured in identity research' (p. 10). The authors observe the role that personal and social identities play in each other's construction. On the one hand, 'personal identities necessarily draw on available social discourses or narratives about who one can be and how one should act' (p. 11). Furthermore, self-conceptions emerge and develop in reference to a range of associations, roles and behaviours that tie the individual to his or her social surroundings. On the other hand, social identities cannot be formed without individuals that engage in action and interaction that are informed by some notions of the self. Thus, the two forms of identity are intimately intertwined in a way that makes it hard to examine or understand one in complete separation from the other.

In accordance with this line of argumentation, several researchers have attempted to highlight the common features that personal, social and organisational identities share. Some have done this by stressing the *relational aspects of identity*. As pointed out by symbolic interactionists, personal identity is inherently relational (Sluss & Ashforth, 2007); one's self-conception as a powerful leader can only be achieved with the presence of followers. Social identity is similarly relational; it is through ongoing relationships, interactions and comparisons with various out-groups that the in-group becomes a salient locus for individual identification and attachment. Organisational identities are also relational as they are constructed not only against a backdrop of members' shared histories and experiences but also in the context of multiple interactions in which the organisation is involved with a variety of outsiders such as customers, competitors and suppliers (Ashforth & Mael, 1996; Gioia *et al*, 2000).

Another characteristic of identity in organisations is its *fluidity*. Although much of the literature has played up and focused on the seemingly stable and enduring features of identity, acknowledgement of its potentially changing character can be found in recent research on the topic (Gioia *et al*, 2000). For instance, personal identity is seen as a social construction deriving from changing interactions with others. As Weick (1995) puts it, 'identities are constituted out of the process of interaction. To shift among interactions is to shift among definitions of the self' (Weick, 1995, p. 20). Social identity is also flexible; an individual's representation of in-groups and out-groups is likely to change as features of the comparative and normative context undergo transformations (Cornelissen *et al*, 2007). *Flexibility* is also a characteristic of organisational identity. Changes in the organisation's environment and relationships with other organisations are likely to require modifications to the way members interpret what is central and distinctive about their organisation. That is, organisational changes will require members to actively reinterpret and develop new representations to symbolically characterise their organisation (Fiol, 1991).

Two additional qualities that characterise identities in organisational contexts are the role that they play in *informing* individual and collective action and their *embeddedness* in social discourse and communication. First, individual actions are performed by actors with certain dispositions and preferences that derive from their self-conception. Likewise, social identity orientates the behaviours of individuals based on inter-group comparisons and relationships and the construal of social information. Organisational action is informed by organisational identity that provides a basis for sense-making and renders a particular repertoire of behaviours appropriate; a 'green' organisation is likely to take certain actions to reduce resource consumption and be associated with relevant industry and environmental groups to justify its green identity.

Second, most researchers agree that identity is produced and reproduced through ongoing communicative activities that take place within and across people and organisations. For example, social construction theorists maintain that personal identities are created, negotiated and changed through ongoing interactions among multiple actors (Alvesson *et al*, 2008). Organisational identity is also a product of social communication; organisational members negotiate, through continuous interactions, a shared symbolic representation of their organisation that gives a sense of meaning to the organisation's actions, objectives and existence. That distinguishes the organisation from other social entities in its environment (Gioia, 1998; Gioia *et al*, 2000).

To sum, the concept of identity provides a lens for studying how organisational members give meaning to their experiences as a basis for individual and collective

action. Therefore, it offers an opportunity to explore the interrelationships between the symbolic and the concrete organisational domains, as well as to examine the reciprocity of micro activities and macro phenomena. The recognition that identity is a foundational notion that is essential to understand multiple organisational processes and experiences is evident in the wealth and diversity of research that has employed the concept. In what follows, the paper examines the utilisation of the identity concept in information systems research and characterise its application around two themes.

The interrelationship of technology and identity in the context of systems implementation

The drivers and impediments to successful implementation of information systems have long been of interest to researchers. The manner in which identity issues may be involved in this process has been explored in a number of studies. Van Akkeren & Rowlands (2007) examined the assimilation of new information and communications technologies in a radiologist practice and drew on social actor theory to analyse the relationships among the radiology practitioners, the technology and the context. The findings from the case study showed that user-identity can both inhibit and enable assimilation. Gal *et al* (2008) studied the implementation of three-dimensional technologies into the architecture industry. They proposed a model to outline the relationship among information systems, information infrastructures and organisational identities and suggested that the systems help to form organisational identities and enable cross-organisational change. Similar to Gal *et al*, Alvarez (2008) also emphasised the co-construction of identity and information systems and argued that technology, structure and identity are mutually constitutive. Critically examining the implementation of an enterprise system, Alvarez discussed users' power relations, experienced loss of autonomy, isolation and fragmentation during the implementation process. Barrett & Walsham (1999) studied the implementation of an electronic trading system in the London Insurance Market and drew on work by Giddens to examine its impact on users' self-identity. Finally, Barrett & Scott (2004) also utilised Giddens' concept of self-identity and examined how reflexive self-identity is impacted by increased globalisation and technology use during the adoption of an e-trading system.

Identity in online communities

In recent years, information systems scholars have mostly studied identity in the context of online interactions and communities. For instance, Forman *et al* (2008) looked at the relationships between online shopping and consumers' identity. Drawing on theories of information processing and social identity theory, the authors suggested that self-disclosure of consumers' identity affects the behaviour of other shoppers and is positively related to sales. Ma & Agarwal (2007) studied the impact of community infrastructure design and identity verification in computer-mediated communication. Their findings suggested that identity verification is positively impacted by technology artefacts and leads to satisfaction and knowledge contribution in online communities.

A number of researchers tried to explain what makes online communities successful. Yuqing *et al* (2012) studied the success of online communities by examining how they garner member attachment. They found that strengthening members' group identity can increase their attachment to the community. Strengthening members' interpersonal bonds was found to have a similar, albeit weaker, effect. Highlighting the importance of 'we-ness' to online communities, Fayard & DeSanctis (2010) drew on Wittgenstein's concept of 'language games' to explore how participants of two online forums constructed a collective identity through discursive practices. Similarly, Sarker & Sahay (2003) proposed a theoretical model that relates the concepts of communication, virtual team development and collaboration to understand how virtual teams develop over time. They suggested that the development of an 'integrative identity' across teams is an enabler of successful collaboration. Kim *et al* (2012) examined what motivates people that participate in online communities to purchase digital items. They found that a decision to purchase such items is driven by participants' desire for online self-presentation. Finally, Dickey *et al* (2007) studied how customers and customer service representatives build a shared context in online chat communication. They viewed identity as the interpretations that customers have of the company representatives' appearance in the chat session. They described how improvements in peoples' articulation of intention and creation of a shared frame of reference may be valuable in enabling coordination between customers and customer service representatives.

Having explored research into the notion of identity and its use in information systems research, the paper next describes the concept of identification and outlines the main issues around its application in the information systems literature.

Researching identification

A recent paper by Smith & McKeen (2011) notes the increasingly important role that identification plays for organisations and enterprises. With growing numbers of services being provided online, from commerce transactions to accessing organisational data assets, organisations 'must trust that they can identify and authenticate the customers, businesses, employees and third parties using them' (p. 170).

Identification schemes are intended to increase trust or assurance about identities, particularly online (Bernat, 2011). Cameron (2005), for example, sees the role for digital identification schemes as preventing a loss of trust and enabling internet users to go forward with 'deep sense of safety, privacy and certainty about who they are relating to in cyberspace' (Cameron, 2005, p. 1). He then defines

a digital identity as a *set of claims* 'made by one digital subject about itself or another digital subject' (Cameron, 2005, p. 4). It is these claims that the *relying party* needs to decide whether to trust and act upon or not.

These claims might be detailed claims that allow the digital subject to be *identified* ('I claim that my name is Elizabeth Yap') or simply be *authenticated* without necessarily being 'identified' ('I claim to be over 18 years old', 'I claim to have special powers obtained in level 3 of the online game'). The level of assurance needed to support the claim will vary from situation to situation and an effective organisational strategy involves a risk-based assessment of the level of assurance required for a specific transaction. This will include consideration of how that assurance can be obtained (e.g., Cabinet Office, 2012).

For example, when subscribing to an online newsletter, the relying party has no particular need to verify that the subscriber is really called Elizabeth Yap, yet if this were an application to receive the tax refund due to Elizabeth Yap a higher level of assurance to support the claimed identity would be needed to prevent a fraudulent payment being made. Similarly, the evidence base for this assurance can vary. For 'official' records like name, citizenship or date of birth, the basis for the claim might be found in official government records (Lips *et al*, 2009), 'lifestyle' records that provide assurance as to where someone lives and what transactions they regularly complete can be provided by banks, utility firms and phone companies. In contrast, assurance about special powers obtained in the online game would only be relied upon if they come from the game provider.

Although the claims can refer as much to technological objects (is this website really the website of the publisher of this journal?) as it does human subjects, the scope of this special issue is on human identification systems. For studies that relate to identifying technological objects, see, for example, Bose *et al* (2009).

Identification infrastructures

With the growing importance of identity and trust issues for online transactions, there is a realisation that the development of bespoke identification mechanisms to support trust online is unduly costly and identification schemes are increasingly becoming interoperable to allow for cost savings following the reuse of existing systems.

This interoperability introduces its own research and management challenges and it can be argued that systems for identification are best conceptualised as *identification infrastructures* as they share many of the characteristics of information infrastructures that have been studied by information systems scholars (Monteiro & Hanseth, 1995; Star & Ruhleder, 1996; Ciborra & associates, 2000; Darking & Whitley, 2007; Henfridsson & Bygstad, 2013). For example, it has been shown repeatedly that infrastructures often constrain future actions in unexpected ways.

Thus many identification infrastructures seek to reliably link an individual to some unique identifier, such as a social security or tax identifier in the public sector or a unique employee or customer identifier in the private sector. Nevertheless, any identification infrastructure will always operate in the context of other existing administrative records and identifiers. Thus an identification infrastructure based around social security identifiers might co-exist with tax records that use their own distinct index or an enterprise-wide identifier might co-exist with departmental identifiers.

Given the departmental silos that often exist in modern organisations, considerable effort and resource will be required if it is decided that one index will become the *de facto* identifier for the whole organisation. For example, Dunleavy (2005) notes that the U.K. tax ministry required taxpayers to use that ministry's own taxpayer number rather than their social security number when filing tax returns because the tax authority was not prepared to pay the social security department for the use of their identity data.

Significant resources may also be consumed from what appears to be the relatively low-level task of redesigning existing systems to use identifiers with different formats. For example, Eriksson & Agerfalk (2010) describe the situation where student identifiers in Swedish university records systems needed to be updated to allow the system to register international students. These changes were estimated to cost at least €776,000 while more wide-ranging changes to the format of identifiers in other associated systems could cost anywhere between €4,100,000 and €46,000,000 to implement depending on the technical solution chosen.

Even if these practical issues are addressed, the study of information infrastructures suggests that during the periods of transition there will need to be two systems in existence, with two sets of processes for handling identification – one for those within the new system and one for those still in the old system. Infrastructures are never built from scratch and they can never be changed all in one go. At a trivial level, switch-over is always going to take a finite time and, for most systems, the introduction of a new infrastructure will be phased over a period of months or even years, as new equipment and processes are introduced, with associated periods of retraining and organisational adjustment.

This means that any infrastructure development project will never cover the whole of the infrastructure, but rather will need to be developed in conjunction with the constraints arising from existing aspects of the infrastructure. It is therefore very difficult to determine in advance what the boundaries of the infrastructure will be.

Infrastructures must be able to cope with the dual constraints of local variety and centralised planning. Issues of standardisation and interoperability become significant so that identification credentials can be read across the whole of the identification infrastructure (Mahler, 2013). As a result, for example, machine readable travel documents are based on open standards (ICAO, 2003).

Issues of path-dependency also apply, with self-reinforcing mechanisms often preventing much-needed change

from arising. This means that once the infrastructure is initialised, unless it is very carefully designed and managed, it will be increasingly difficult to make significant changes to it. Carefully designed infrastructures can be modularised and abstract key components but there is still a risk that some design decisions are not as technology neutral as first thought and will still constrain future decisions in unexpected ways (Whitley, 2013). Similarly, other features of the scheme, such as the use of biometrics (see below), might result in significant management challenges as biometric technologies advance (Carter, 1998; Bowyer *et al*, 2009) including the risk of needing to recollect large numbers of new biometrics from the user population. As a result, most key decisions about infrastructures have to be taken at times when knowledge about the factors that are affecting the decision is limited. Similarly, there is often a constrained period of time when such decisions can be taken (Ciborra & Associates, 2000).

Another important challenge faced by infrastructures relates to the question of paying for them. It is important to understand the purpose of charging. Charges are sometimes used merely to manage an infrastructure to ensure against abuse, or to pay for processing charges and possibly for revenue generation. For example, should relying party users of the infrastructure simply pay for the use of a service that verifies a particular individual, or should they also contribute towards the ongoing maintenance of the system from which they receive these indirect benefits? Should such contributions also cover the cost of enrolment into the system, or is this cost to be solely associated with the individual who obtains the identification credential? As the infrastructure becomes increasingly widely used, further issues of costing arise. Should the cost of use be fixed over time, or should the costs be based on some estimate of long-term stable usage patterns? Can costing models incorporate potential increased usage that arises from unexpected uses of the identity scheme? The relatively low take up of applications that use the features of identity credentials, such as digital signing etc., across the world is evidence that the problems of valuing identification services and providing a resilient business models have not yet been solved (IAS Project, 2011).

More generally, identification mechanisms raise significant policy, technological, managerial and societal questions that have been studied by information systems researchers among others, at different levels of abstraction and adopting a diverse range of research approaches (Halperin & Backhouse, 2008). A large proportion of this literature focuses on national identification schemes but the issues that are raised have counterparts in enterprise-level schemes. The remainder of this section reviews these questions in more detail.

Policy questions

The decision to introduce or upgrade an identification infrastructure is one of the most important policy decisions taken by an enterprise or the state (Whitley & Hosein, 2010a) and there can be significant administrative and social consequences of their use (Bennett & Lyon, 2008; Kerr *et al*, 2009). There are many reasons for doing this. Commonly espoused reasons include simplifying citizens' access to public services, increasing trust in online transactions, seeking to address various forms of fraud, terrorism prevention and managing borders (Koops *et al*, 2009). In the private sector, the identification infrastructures may seek to manage and control employee access to resources (both physical and electronic) and monitor their location and performance (Seltsikas & O'Keefe, 2010). With broad reasons being espoused for an identity policy, there is a real risk of unclear focus, scope-creep and even incompatibility (Whitley & Hosein, 2008a). For example, a policy to simplify e-government interactions might not be particularly effective at addressing illegal immigration; a policy to use biometrics to record when employees check in and out of work may run counter to moves to empower employees.

National schemes are typically intended to provide a secure means by which citizens can assert claims about their identity (Barnard-Wills & Ashenden, 2011). For example, although passports have their origins in travel documents confirming a right to leave a country, they are nowadays also seen as high integrity documents that confirm citizenship and are evidence to support a claimed right to work in a country. Driving licences are another form state-issued credential that is frequently used for these purposes. Increasingly, national identity schemes are also being used for online transactions with e-government services (Bernat, 2011).

National identity schemes include the failed U.K. national identity scheme (Beynon-Davies, 2011), the new Indian Aadhaar scheme (Ramakumar, 2010; Krakovsky, 2011; Romero, 2012) and the ongoing U.S. REAL ID initiative (Rotenberg, 2006; Gates, 2008) as well as existing identity schemes found in many countries (see, e.g., the reviews by Arora, 2008; Bernat, 2011).

A distinguishing feature of state-issued identity credentials (historically often taking the form of a physical book or plastic card) is the important role of identity proofing/verification that takes place before the credential is issued. Traditionally, an individual's claims about name, citizenship etc. were checked against existing public and private sector records such as voter registration lists, birth registers, tax records or credit reference agency databases (Lips, 2013; Cabinet Office, 2013b). For private sector enterprises, other than for situations that require detailed personnel vetting, the proofing process typically piggybacks on existing national schemes. For example, before hiring a new employee the individual may need to demonstrate a legal entitlement to work that is supported by a suitable passport or work permit.

These schemes raise challenging issues about technology adoption and use. Considerable research evidence suggests that adoption is likely to be influenced by the perceived usefulness and ease of use of the technology (e.g., Davis, 1989; Davis *et al*, 1989). That is, technology

that is perceived to be useful and easy to use is more likely to be adopted than technology that is not perceived to be useful or which is difficult to use.

An important nuance in this literature, however, relates to whether the use of the technology is compulsory or voluntary (Wu & Lederer, 2009). That is, in an environment where use of the technology is compulsory, issues of perceived ease of use and perceived usefulness are likely to be less significant. In addition, it is often assumed that understanding the voluntariness of technology usage is unproblematic (Moore & Benbasat, 1991). In many cases, however, identity credentials become a *de facto* part of many transactions with government and private sector organisations even if there is no legal compulsion to possess or carry them (Perri 6, 2005). For example, to address concerns about identity fraud individuals may need to show their identity credential when paying using a credit card. Such cases are nominally voluntary but are effectively compulsory and it is unclear whether existing research results about the voluntary adoption of techologies apply to them.

Technological issues

Technological decisions about the design of identification systems have also been widely studied in the literature. These can range from choices between using contact and contact-less smartcards to decisions as to whether to verify identity against information held on the card *vs* checking identity claims against a centralised database.

Another important technological choice relates to the use of identifiers. As noted above, changing the format of an identifier can have significant cost implications for system and process redesign (Eriksson & Agerfalk, 2010). Further problems arise if the identifier is in the form of a 'smart number', for example, incorporating gender, date of birth or place of birth in the identifier code. In addition, cultural sensitivities surround particular identifier patterns where numbers like '666', '4' or '8' might be popular or problematic according to context.

Similarly, it is possible to use single or multiple identifiers across a range of services (Otjacques *et al*, 2007). The widespread use of a single identifier, such as the social security number in the U.S., is known to be problematic and potentially increases rather than reduces fraud (Garfinkel, 1995; Berghel, 2000; Froomkin, 2009).

Within Europe, France explicitly does not use a single identifier to link government records across departments (Whitley & Hosein, 2008b). Hungary and Germany explicitly ban the use of a single identification number for citizens, citing data protection concerns, while France, Lithuania and Italy are very restrictive and limit the data directly linked to the identification number to a minimal data set. Similarly, countries like the Czech Republic do not allow shared databases across government departments (Otjacques *et al*, 2007).

The Austrian e-government initiative has introduced a novel technology-based solution, where all Austrian citizens are registered on a national Central Register of Residents but have a variety of identification numbers that link to the central records via sector-specific tags and strong encryption algorithms (Otjacques *et al*, 2007; Aichholzer & Strauss, 2010).

Biometrics are another important technological component of many identity schemes (Mordini & Massari, 2008). Biometrics can include face, signature, fingerprint and iris patterns (Daugman, 1998; Kabatoff & Daugman, 2008; Neyland, 2009; Shaikh & Rabaiotti, 2010) and technological processes transform the image of the biometric into a numerical template which can then be automatically compared against other biometric templates although expert manual checking of matches is also often required (Davis & Hufnagel, 2007).

Some authors see biometrics as ideal ways of linking an identity back to an individual (Jain *et al*, 2004; Jain, 2007; Kabatoff & Daugman, 2008; Bromby, 2010). Other research, however, sees the role and effectiveness of different biometric techniques as problematic (Bowyer *et al*, 2009) and raising specific policy issues (Hornung, 2005). These include systematic exclusion issues that can arise when individuals are unable to provide usable biometrics (Gates, 2005; Wickins, 2007; Magnet, 2011).

The apparently clear link between biometrics and a unique physical identity has also been questioned, for example, in the case of transgendered individuals (Currah & Mulqueen, 2011; Martin & Whitley, 2013).

Cryptographic techniques, enabled by smart-cards and other secure chip-based processes (such Subscriber Identity Module (SIM) cards) offer the opportunity for citizens to make use of digital signatures in public and private transactions. For example, the Estonian Digi-ID is seen as an exemplar in that in addition to being an identity card that can be used for identification purposes online it can also be used to provide electronic signatures (Estonia Digi-ID, 2013).

Similarly, different technological implementations of an identity credential can offer different levels of privacy protection for citizens (Van Alsenoy & De Cock, 2008; ENISA, 2009). Indeed, Birch (2009) argues that technological infrastructures can deliver identity solutions that deliver far more than politicians, professionals and the public imagine. One instantiation of this is the privacy-enhancing identity credential offered by Touch2id, a U.K. company that incorporates fingerprint biometrics to address a specific policy challenge namely proof of age claims (for the purchase of age-restricted products such as alcohol). As Birch (2009) notes, in such situations, the only thing the relying party needs to know is whether the person is over the required age or not. It is not necessary to know the person's name, address or even their date of birth.

Having enrolled with Touch2id (which involves generating the unique fingerprint biometric template and storing it on a smart-card, Near Field Communication service or mobile phone 'sticker' alongside a verified date-of-birth and other system information), the young person is free

to use this credential to prove their age. For example, when entering a bar, they present their credential to a reader device and present their fingerprint on the reader, where a second fingerprint biometric template is generated from the presented fingerprint. If the templates match and the date-of-birth stored on the chip confirms that the person is old enough to be served on that day, a green light flashes and sound is generated confirming that the person can be served.

Touch2id therefore provides a form of 'zero-knowledge proof' for the claim that an individual is old enough to be served. It does so without revealing anything other than the veracity of that claim. The bar owner checking whether someone is allowed to be served can do so with a sufficient level of assurance in this claim (the date-of-birth has been verified and the person presenting the credential is the person that it was issued to) and without generating an archival record of who visited which bars when (Whitley, 2013).

Managing and controlling identity schemes

Given the role that identity schemes play in maintaining and enhancing trust, particularly in online transactions, it is increasingly important that the schemes are securely managed and controlled (Smith & McKeen, 2011). For example, as possession of a valid passport is accepted as proof of citizenship, entitlement to public services and the right to work, particular care must be taken to minimise the risk of passports being incorrectly issued to individuals and of plausible fake passports entering circulation (e.g., De Cock *et al*, 2008). This implies that security and management controls must be in place throughout the identification life cycle.

Despite having their origins in financial audit and control, these concepts are increasingly being applied to the management of information systems in areas such as financial reporting and data quality (e.g. Bai *et al*, 2012; Li *et al*, 2012). Many of the same insights can apply to management controls around identification data, for example, balancing the need for regular external audits to maintain confidence in the process with the costs and disruptions associated with the auditing process.

For example, the means by which an individual enrols into an identity scheme needs to be carefully controlled to ensure that only eligible individuals are enrolled, that any biometrics are taken properly (Rehman-Greene, 1998) and that the claims they make to support their enrolment are checked to a suitable level of assurance (e.g., Cabinet Office, 2013b). Many of these checks rely on the integrity of the original 'breeder' documents (Berghel, 2006; Collings, 2008) in that if the underlying records contain errors or are incomplete, the risk of fraud or incorrectly issued credentials increases.

The existence of suitable management controls should prevent cases such as one reported in relation to the Indian Aadhaar scheme where a coriander plant was issued its own unique identity number (*The Tribune*, 2012).

Similar controls need to be in place for the secure production and delivery of identity credentials such as cards or passports. The production process typically includes features that make them tamper evident and difficult to fake. For example, the U.K. government has issued a 16-page booklet that provides details of (some of) the security features that can be checked in a British passport including laser perforated numbers, hologram patches and features that can only be seen in ultra violet light (HM Passport Office, 2011) although these features only provide protection if they are actually checked.

With identification infrastructures increasingly using cryptographic measures on their smart chips etc., the management challenges of building and maintaining large-scale public key infrastructures (PKI) remain very real (Backhouse *et al*, 2005). Indeed, for many countries and enterprises the technical challenges of managing complex components of the identification infrastructure like PKI means that the process is frequently outsourced. Despite this, not all public and private sector enterprises have sufficient internal capabilities to effectively manage such outsourced relationships (Willcocks *et al*, 2007; Cordella & Willcocks, 2010; Weigelt, 2013).

From the perspective of individuals, many countries place specific legal restrictions on whether data can be shared without the individual's consent or processed outside that country's legal jurisdiction. Any proposals to outsource aspects of the identification infrastructure therefore need to include consideration of these issues (European Parliament, 2012).

Societal questions

Societal concerns about identification schemes are among the most widely studied in the information systems and related literatures. Indeed, failing to address legitimate concerns about the nature and scope of an identification scheme can result in limited take up or even abandonment of the scheme, with associated reputational consequences (Whitley & Hosein, 2010b).

Some of the most critical literature emerges from the field of surveillance studies. These studies seek to understand implicit and explicit surveillance capabilities of technological systems where the watching over of individuals goes well beyond idle curiosity (Lyon, 2007; Ball *et al*, 2012). In the context of identification systems the collection edited by Bennett & Lyon (2008) provides international perspectives on surveillance and identification. Similarly, Lyon (2009) specifically highlights the role of what he describes as the 'card cartel' whereby big business implements identification systems for enterprises and countries and, in many cases, even helps create the market for such services (cf. Pollock & Williams, 2009).

Concerns about surveillance abuses by government have been particularly prominent in certain European countries (e.g., Home Affairs Committee, 2008; FIPR, 2009; Hornung & Schnabel, 2009; European Parliament, 2012). They have been conceptualised as means by which the state might

'govern by identity' (Amoore, 2008). Particularly contentious is the role of identification credentials for recent immigrants (Thomas, 2005; Broeders, 2007; Sadiq, 2009) where constant checking of their identification documents might be seen as a form of profiling and problems issuing credentials might limit their ability to participate in elections (e.g. Atkeson *et al*, 2010).

Other surveillance concerns can arise as direct consequences of technological decisions. For example, the choice to perform identity checks against centralised registers risks leaving detailed audit trails of where and when a particular individual had their identity verified. These records can soon build up detailed behavioural profiles of the individuals concerned (Home Affairs Committee, 2008). Other forms of centralised databases of identity data raise other ethical concerns, particularly in the context of totalitarian states (e.g., Bing, 2009).

The use of biometric technologies is another area that raises complex policy, legal and ethical issues (Alterman, 2003; Hornung, 2005; Introna & Nussenbaum, 2009) particularly in relation to broader ethical questions about privacy and data sharing (Davies, 1998; Sprokkereef & De Hert, 2007). Specifically, many raise the concern that biometrics, unlike passwords, are irrevocable. That is, if the biometric becomes compromised its very nature means that it is impossible to issue the individual with a replacement fingerprint.

Biometrics also differ in how they can be captured and in terms of their association with other activities in society. For example, while face biometrics are widely used and accepted they can be also be captured remotely (and surreptitiously) while iris biometrics need specialist devices to capture them and using fingerprints may carry strong associations with criminality.

These privacy and surveillance concerns, whether founded or not, are likely to affect the choice, take up and use of identification credentials, particularly if individuals have a free choice around their use. These factors have been examined in the information systems in a number of recent studies. For example, Dinev *et al* (2008) report that concerns about government intrusion were related to privacy concerns and affected the willingness to disclose personal information, results echoed by others (Bailey & Caidi, 2005; Lim *et al*, 2009). Other studies have extended the scope to include specific consideration of biometrics in national identity schemes (Ng-Kruelle *et al*, 2006; Li *et al*, 2008).

Given these concerns about privacy and surveillance by the state, an emerging research area surrounds the notion of identity rights. This seeks to understand, from an ethical and empirical basis, what expectations individuals may hold around the use of identification systems (Hoikkanen *et al*, 2010). Indeed, a number of recent identification proposals have explicitly sought to redefine the nature and scope of the infrastructures to address concerns about privacy and surveillance, putting the citizen's needs at the core of the process (Sir James Crosby, 2008; Rahaman & Sasse, 2010; Schwartz, 2011; Cabinet Office, 2013a).

On the interplay between identification and identity

As noted at the start of this review it is often helpful to make analytical distinctions between studies of identity and studies of identification. Nevertheless, in the real world this academic distinction is becoming increasingly blurry and technology is increasing the interplay between identity and identification. This section presents two cases where technology is transforming the interplay between the two. One starts from identification, the other from identity. These are followed by a discussion of future directions for research into identity and identification.

Obtaining legal identity

Individuals in a modern state expect to be able to participate fully in its social, political and economic life. That is, they expect to benefit from the rights and protections that are bestowed by the state including education, healthcare and social security. They anticipate fulfilling their duties like voting and wish to be able to participate in economic activities by having access to banking and credit services, property titles and inheritance. This inclusion often provides the foundation for the establishment of social identity, which constitutes that part of an individual's self-conception that derives from his or her membership in particular social groups (Tajfel & Turner, 1979). Through participation in the life of the state, citizens enhance their sense of belonging to it and develop a social identity that reflects the state's perceived nature.

Underlying such citizen participation is the notion of legal identity, namely the recognition by the state that the individual exists and is therefore afforded these various rights and responsibilities. If this legal identity is missing, people can find themselves effectively excluded from many of the basic activities in society and with a diminished base from which to form their social identity.

Thus, despite the concerns about state surveillance outlined above, for many obtaining a legal identity is an important step towards citizenship (Murakami Wood & Frimino, 2009). Legal identity has been defined as 'legal civil status obtained through birth registration and civil identification that recognises the individual as a subject of law and protection of the state' (Harbitz & Molina, 2010). Thus it can be understood to be the combination of factors that enable a person to access rights, benefits and responsibilities.

Legal identity involves the registration and documentation by the state of various forms of personal data as outlined above. Legal identity or citizenship identifies who is subject to the rights and obligations conferred by the state and who is not. Focussing on legal identity highlights some of the ways in which problems with registration can arise. For example, there may be a failure to register the individual either correctly or even at all. It is estimated that 51 million children a year worldwide are still not registered at birth (UNICEF, 2007) as parents may not recognise the importance of birth registration

or the procedures are too difficult to follow. Novel approaches to address these problems include the use of mobile devices to support birth registration in remote rural areas. Incorrect registration of births can cause problems in later life where it becomes impossible to match the adult claiming a particular legal identity to what might have been 'registered' at birth. Other problems can arise when names and details in indigenous languages are transliterated into the form and format required by the identification infrastructure (AllAfrica.com, 2010).

Nevertheless, when legal identification mechanisms are updated and well managed, important questions of national identity can be addressed and can provide significant benefits in terms of social stability and economic development. For example, legal identity in Peru has been the key to participation and inclusion and has contributed to solidify the democracy, particularly following the internal conflicts in the 1980s (Harbitz & Boekle-Giuffrida, 2009). RENIEC (Registro Nacional de Identificación y Estado Civil) is the independent civil registration institution in Peru that has generated high levels of citizen trust. It was created in 1995 after the new Peruvian constitution was approved.

During the internal conflict many local registration offices and associated registration books were burned or vandalised. As a result a number of individuals were left without documentation and consequently extremely vulnerable (Orihuela, 2009). Through the work of RENIEC and associated bodies to re-enable the infrastructure responsible for legal identification, Peru illustrates the interplay between symbolic and organisational domains in enabling all citizens to form their social identity and history as Peruvians.

Extending personal identities

The use of social networking sites has grown considerably in recent years. During this time the focus of social networking use has shifted from platform to platform, for example, from MySpace and Second Life to Facebook and now, increasingly, to Twitter, Instagram etc. This shift seems to reflect a combination of fashion, technological developments and network externalities as much as intrinsic hedonistic motivations for using the services.

In some cases, social networking sites provide an opportunity for individuals to explore aspects of their personal identity in a medium that transcends the physical constraints of the body and affords flexible social interactions across spatial and temporal boundaries. Other social networking sites, such as LinkedIn, are used by individuals to enact a professional identity and develop it by establishing relationships with and seeking endorsement from other professionals in their field. The membership of the same individual in both professional and social networking websites may create tensions between that individual's personal and professional identities and thus require strategies to manage the boundaries between them (Ollier-Mala Terre *et al*, 2013).

The enactment of online identity and management of multiple identities across different online domains is bound together with issues of identification. Many social networking sites invoke a 'real names' policy and disallow the creation of multiple accounts by a single individual (Tene, 2013). Despite this, these sites are now replacing online bulletin boards and multiplayer games as the environment where such identity play takes place (cf. Turkle, 1996). For others, however, having a single, authenticated online identity for social or business purposes is considered essential (van Dijk, 2013). Thus, LinkedIn profiles and their associated endorsements and recommendations become valuable sources of social capital, particularly for employees seeking to change jobs.

Given this emergent value of both the social networking profile and its network of associations, there are growing pressures to use this (social network) data about connections and endorsements as part of the identity proofing processes for more formal identification processes (Martin & Andrade, 2013). The practical and research challenge, therefore, is to determine the level of trust (assurance) that can be given to an individual's social networking profile where that profile has connections and endorsements from other known members of the relevant community as well as personal connections. Other challenges arise from concerns about using private sector rather than public sector data to perform this duty (Lips, 2013).

Particularly significant is the risk of fraud whereby a fake account is set up and becomes linked up with large numbers of other (faked) accounts. Managing the risk of such fake profiles is becoming understood in the context of customer review sites (Scott & Orlikowski, 2012) and social networking identities may be more difficult to fake systematically (e.g. the level of assurance is based not only on the number of connections to other (fake?) profiles but also on the extent to which these further connections have realistic behaviour profiles in terms of activities like posting and commenting).

Situations of online harassment (BBC News, 2013) provide a related context where there is an interplay between concerns of identification and the enactment of personal or professional networking identities. Abusive behaviour in social networking sites is common and may lead to negative repercussions to individuals' online, as well as offline, identity and social status. Although it is currently possible to create online profiles without any form of identity checking, the prospect of formally linking online profiles to verified national identification credentials, as is the case in some countries, is very real. It is recognised that in online discussion and decision-making fora, there are many benefits to allowing anonymous/pseudonymous contributions. The effect of making identification linkages in social networking sites stronger is less well understood and while addressing concerns about abuse and criminality may also have undesired negative consequences.

Future directions for research in identity and identification

Given the wide scope of concepts and their limited application in the information systems literature to date, there are multiple opportunities to use them in future research. This section outlines some research opportunities, starting with identity-related research questions.

Manipulating identity to facilitate organisational processes

In line with the functional tradition, much research treats identity as a tangible construct that can be gauged, assessed and intentionally manipulated through management interventions to achieve desired organisational consequences. For example, some studies suggest that members' level of identification with their organisation impacts decision-making processes, group cohesion (Ashforth & Mael, 1989) and member commitment (Sass & Canaray, 1991). Other research maintains that the emergence of a collective identity influences the way members interpret and react to issues facing the organisation (Dutton & Dukerich, 1991; Gioia & Thomas, 1996) by influencing the importance that members assign to them.

The theoretical framework most often associated with this approach is social identity theory (Tajfel & Turner, 1979). The theory's main premise is that people's identity derives from the groups to which they believe they belong. Because people strive to maintain a positive self-identity, they will tend to favourably compare their in-group to external out-groups along valued dimensions. Applying these ideas to the organisational domain, it has been argued that organisational identity is merely a form of social identity, one that is associated with perceived membership to an organisation (Haslam, 2001). Therefore, one's degree of identification with the organisation provides the basis for a range of organisational behaviours such as leadership, group motivation and willingness to take on organisational roles and exercise collective power (Turner, 2005).

Opportunities for researchers in this approach are varied. For example, one could look at the role of technology in facilitating the creation and maintenance of organisational identification among group members. As identification with the organisation is assumed to have a decisive influence on a range of organisational actions, being able to control and manipulate the identification process becomes an important managerial issue. Therefore, research that looks at the way technology can assist in accomplishing this in different organisational situations, such as geographically distributed or virtual teams, can be particularly valuable.

Another research possibility lies in examining the impact of members' identification levels on their willingness to accept new technologies. Technology acceptance research is one of the most substantiated in the field. This area can be considerably enhanced by examining how the emergence and strength of social identities influence the propensity of users to adopt and use a new technology.

Understanding the impact of organisational processes on identity

Whereas the research described in the previous section aims to target and utilise identity to produce effective organisational behaviour, another line of inquiry is primarily interested in understanding human experience in organisational settings. Rather than directly serving organisational interests, such inquiry looks to gain in-depth insights into people's subjective reflections on who they are and what they do in the context of the organisations in which they work and in relation to the technologies that they use (Alvesson *et al*, 2008). This approach focuses on how people weave organisational narratives with personal experiences to construct identities that provide a sense of meaning and continuity over time and across geographical locations (Ravasi & Schultz, 2006). This construction process is often referred to as 'identity work', a term that is meant to emphasise the continual and dynamic nature of identities in organisational settings and their capacity to change and adapt to accommodate transformations that take place within or outside the organisation.

This idea is demonstrated in a number of studies such as Fiol's (2002) examination of an organisation named Tech-Co. During the 1970s and 1980s Tech-Co had a stable organisational identity as an engineering-driven data storage company. However, during the 1990s, the computer storage industry as a whole was undergoing significant changes from a hardware and engineering mindset to a mindset of information management and storage solutions. Fiol followed the transformation in Tech-Co's identity as the company attempted to adapt to the changes in its environment (Fiol, 2002).

Some research that used the concept of identity is similar in nature. For instance, Lamb & Davidson (2005) described the transformations in the professional identities of groups of scientists associated with the introduction of a new information system. Similarly, Gal *et al* (2008) studied the transformations in the identity of an organisation in the American architecture industry as it adopted new systems while Walsham (1998) and Barrett & Walsham (1999) explored the links between the introduction of new information and communications technologies and changes in the identities of groups of professionals in the London Insurance Market. This kind of research can enrich our understanding of how individuals, groups and organisations incorporate technology-enabled changes in their environment into ongoing identity work; how new technologies get interpreted and feed into the way people perceive themselves and their organisations; how ongoing enactments of organisational interactions, practices and identities are influenced by the introduction of new technologies; and what role existing identities play in sense-making processes of new technologies.

The interplay between technology, identity and power

A third approach that incorporates identity issues in research focuses on power relations and repressive discourses that exist within and across organisations. These relations and discourses impose certain normative demands, behavioural scripts and cognitive frames that shape individual, group and organisational identities, both explicitly and implicitly. Drawing on a critical research perspective, this approach challenges some of the basic assumptions that characterise the previous two approaches outlined above, most importantly, that individuals and groups freely construct their identities and (challenging the first approach) that these identities will have beneficial outcomes both for the individuals involved and the organisation (Alvesson *et al*, 2008).

A prominent theme in critical identity research is managerial interest in controlling employees through the regulation of their identities. Efforts to establish a rigid organisational environment that funnels identity construction in specific ways are given prime consideration. Attention shifts to the role that organisational elites play in generating discursive regimes and material arrangements that pose strict limitations on identity construction in ways that are deemed congruent with broad managerial objectives. For example, discourses of quality management, service management and knowledge management provide a rich vocabulary and conceptualise the organisation and its relationship with its members in ways that form and define certain identities, such as 'the knowledge worker'. Identities can also be constituted by reference to their location within a broader organisational or inter-organisational scheme and in terms of their relationships to others. For instance, in a study of an advertising agency, Alvesson found that reference to other agencies as amateurish and insincere tended to be interpreted as communicating professionalism and honesty as desirable attributes to be possessed by members of the researched agency (Alvesson, 1994).

Identity research in information systems that adopts a critical stance can build on existing work in the field that has examined the repressive impact of technology on people's privacy (Zuboff, 1988), capacity to exercise their agency (Kallinikos, 2004) and on the way organisational action and discourse are induced through the implementation of new technologies (Doolin, 2002, 2003). In addition, there are also fruitful insights from the critical literature that examines the surveillance capabilities of identification mechanisms. Future research can examine how systems are used to impose certain discourses that facilitate the construction of particular identities; the role that they play in the distribution of material and symbolic resources within and between organisations and the way these resources are used to construct different identities; and the mechanisms through which information systems structure communicative activities within and between organisations and how these communicative activities (that may be power-laden, asymmetrical, or exploitive) are incorporated into identity construction processes.

Researching the complexities of identification infrastructures

Identification also raises many areas of research that can be of interest to information systems academics. Of particular note is the extent to which themes which were kept separate in this review are inextricably intertwined and co-producing.

For example, the use of biometrics in an identification scheme may be driven by a particular policy agenda (keeping each person's identity unique) but this has significant implications for the technological design of the scheme (what kinds of biometrics will be collected? will the biometrics be held on a smart-chip or only accessible on a centralised database?) that themselves raise management and control issues (how to ensure that the enrolment of biometrics will securely link the biometric to the individual) as well as societal concerns (how will the user population react to the choice of biometrics used by the scheme?).

In the same way, identification infrastructures that are intended to address specific societal and policy concerns, for example by being privacy friendly might be dependent on strict enforcement of both technological and organisational controls including audit to ensure that privacy requirements are adhered to.

Identification systems therefore provide distinctive environments for studying emerging issues in existing information systems research. For example, there is a growing body of research into the design of effective security control mechanisms and why they are often ignored. This research can be applied to the identification life cycle.

More generally, the scope and reach of identification infrastructures challenge information systems researchers to assess adoption intentions that apply to whole populations and not just subsets based on university students and other digital natives. With increasingly ageing but online populations, the usability and convenience of identity credentials also needs to be studied carefully.

Sensitivity to societal concerns, particularly regarding privacy and surveillance, raise novel methodological research challenges. For example, while it is common to use samples of 'regular internet users' or students for many studies (Compeau *et al*, 2012), individuals with strong views on privacy might explicitly choose not to participate in such studies, leading to significant bias in reported research results (Haggerty & Gazso, 2005).

Another methodological challenge relates to the interplay issues alluded to above. Information systems researchers are only beginning to grapple the analytical study of large, complex systems that identification systems typify. There is considerable scope for a more fruitful exchange with related disciplines (such as public administration and management) which have more experience with this kind of complexity but typically downplay the role of the technological artefact (Dunleavy *et al*, 2006).

Identification schemes are not restricted to national schemes and there is far less published research that

explores the interplay of policy, technology and management questions around identification at the organisation level. For example, there is a need for research similar to that of Eriksson & Agerfalk (2010) that details the practical cost implications of changes to existing systems, such as changing the format of identifiers or upgrading credentials.

Given the significant contributions that information systems researchers have made to the study of trust in online applications, the development of new forms of identity credential at the organisational or national level provide ideal opportunities for studies of changing trust perceptions and adoption/non-adoption intentions, particularly in involuntary and pseudo-voluntary scenarios. For example, how do measures to improve the registration of legal identities transform notions of trust in government?

A second trust-related issue focuses on the trust that institutions can place on online data. With individuals spending increasing amounts of time online the evidence base for understanding the extent to which an online persona (such as a Facebook, LinkedIn or Twitter profile) might be trusted (e.g., as part of the identity proofing process) or faked is growing significantly and is open to large-scale data analyses.

Biometrics are relatively under-studied by information systems yet with fingerprint biometrics increasingly finding their way into consumer products alongside their wider use in enterprise environments, up-to-date studies of consumer attitudes to biometric systems is urgently required.

Finally, from a management perspective, the use of advanced identification systems introduces novel risks and liabilities, such as those associated with zero knowledge proofs and third-party accredited credentials. Understanding the commercial and administrative responses to these risks offers another research opening in identification-related research as does consideration of audit and compliance mechanisms.

Explicitly considering the interplay between identity and identification opens up new research agendas and this will be illustrated in relation to the papers presented in the special issue (see below).

Preparing the special issue

As the preceding sections have illustrated questions of identification and identity cross many disciplinary boundaries and challenge the arbitrary distinction between academic research and real-world practice. The two special issue editors (Whitley and Gal) therefore decided that the special issue be supported by an International Advisory Team that drew on specialists both from academia and those whose professional work relates to practical issues of identity and identification (see Table 1). The advisory team was truly international in scope, coming from all three AIS regions although we were unable to achieve a perfect gender balance in the final team. Members of the advisory team were invited, and encouraged, to submit papers to the special issue and a number did so.

A total of 51 papers were submitted to the special issue, although of these 11 were completely out of scope for the special issue (and even the journal itself – an interesting case of mis-identification?). Thus, 40 papers were suitable for being sent out for review. Each of the editors managed the reviews of papers within their area of specialisation (Whitley for identification, Gal for identity) unless there were actual, or possibly perceived, conflicts of interest, in which case the other special issue editor managed the review process for the paper. The editors checked the papers for suitability (and desk rejected a further four papers) and identified appropriate reviewers for the remaining papers with each paper being reviewed by three reviewers. These were drawn from the advisory team and from the other authors submitting to the special issue and other academics. In addition, a number of papers were sent to industry-based experts for their assessment of the 'real-world' contribution of the research (particularly among the 'identification' papers). These experts were frequent commentators and authors of influential industry and governmental reports in the identity/identification area questioning the claims made by some that the rigour/relevance divide between academia and industry cannot be bridged (Kieser & Leiner, 2009).

Twenty-seven papers were rejected after the first round of reviews leaving nine papers in the review process. The authors of these papers were invited to a special author workshop that was held in Helsinki before ECIS 2011. The workshop provided an opportunity for authors to meet with the editors of the special issue and took the form of an interactive workshop.

Each author gave a brief presentation of their paper covering what the paper is about (topic and research methods used rather than detailed results) as well as the key concerns raised by the reviewers and how the authors were planning to address them as well as any concerns that they would appreciate feedback on. Each presentation

Table 1 International advisory team (affiliations correct at time of special issue call)

James Backhouse, London School of Economics and Political Science, United Kingdom
Richard Baskerville, Georgia State University, United States of America
Mia Harbitz, InterAmerican Development Bank, United States of America
Brian E. Mennecke, Iowa State University, United States of America
Benoît Otjacques, Lippman Research Centre, Luxembourg
Boriana Rukanova, Free University of Amsterdam, The Netherlands
Suprateek Sarker, Copenhagen Business School, Denmark
Ulrike Schultze, Southern Methodist University, United States of America
Philip Seltsikas, University of Sydney, Australia
Matt Smith, International Development Research Centre, Canada

was followed by a discussion and feedback session including comments from editors of the special issue as well as from the other authors. In addition, the then *EJIS* editor-in-chief Richard Baskerville spoke about what makes a successful *EJIS* paper.

Six papers were presented at the workshop and the authors of the remaining papers were offered the same opportunity to discuss their proposed revisions with the special issue editors via email.

Following the workshop, the revised papers were reviewed again and, finally, the four papers that completed the review process received final guidance from the *EJIS* editor-in-chief Frantz Rowe before being formally accepted. A number of other papers that didn't make it through the *EJIS* review process have, nevertheless, been published elsewhere.

Papers in the special issue

The papers selected to appear in the special issue reflect the breadth of information systems research in identity and identification. There is a paper about consumer attitudes to identification technologies and one about identity in online communities, a paper about the role of technology for organisational identity and one about technology assimilation and personal identity. The papers also present a diverse range of research methods including choice experiments, case studies, interviews and photo diaries. Finally, the studies are situated in a range of different locations, including samples of German internet users, Second Life entrepreneurs, employees of a French mobile phone and internet service provider and American integrated criminal justice information systems. In addition, this section uses these papers to illustrate further opportunities for research into the interplay between identity and identification.

The paper by Roßnagel *et al* focuses on identification. In an era when service providers like Facebook and Google are used to logon and access social networking and e-commerce sites, the paper seeks to understand user demand for key features of identification services that are not necessarily provided by these 'free' services, for example enhanced privacy and security capabilities. The paper presents a choice-based conjoint analysis of willingness-to-pay for features of identification credentials. The paper explores how willingness-to-pay varies according to the level of privacy and security offered and the application area. The authors studied the willingness-to-pay of German internet users; German attitudes to privacy and security are inextricably linked to their shared history. This potentially makes Germans more sensitive to the choices in the experiment than other groups. Their research found that options where privacy and security concerns were handled by trusted intermediaries were preferred to those where the users themselves control the use of their data. Similarly, sophisticated security and privacy features appear to be valued more by their developers than their potential users.

Willingness-to-pay is relatively under-utilised as a research technique in information systems yet offers the potential for important insights about factors that will affect the adoption and use of new technologies. One interesting way of developing this research stream would be to extend the implicit assumptions about the nature of the German sample to incorporate more explicitly constructs relating to personal or organisational identity as a way of refining our understanding of willingness-to-pay for particular (identification) technologies.

The study by Leclercq-Vandelannoitte stays in Europe but her study takes a longitudinal perspective to explore the technology assimilation process in a French telecommunications company, whose technicians were equipped with a global positioning system (GPS) device in their cars and a smartphone with scheduling software to plan their assignments, based in part on their current location. She adopts a Foucauldian perspective on organisational discourses to understand the technology assimilation process and identifies three key discourse processes. The first relates to the discourses that are imposed to facilitate the construction of the workers' ascribed identities, the second describes the ongoing discourses that influence the workers' self-perceptions and the third is the process of technology assimilation that results from organisational politics. For example, while the use of the GPS system was promoted in terms of 'role enhancement' and 'empowerment' for the technicians, many saw them as a subtle mechanism of surveillance and practice standardisation. Over the period of assimilation of the GPS technology, the paper finds that attitudes and identities shifted, confirming the fluidity of identity and its evolution over time. For example, some ended up accepting the use of GPS as a way of enhancing their identity as professional technicians while others saw their resistance to the way the GPS was implemented as reaffirming their identity as rebels.

The integration of classification systems by means of discursive practices can have a profound effect on people's identities. Such practices name people, assign them to social categories and regulate their subjectivities. As Leclercq-Vandelannoitte's paper discusses, these practices aim to form people's identities by assigning them to predefined social slots. Once discursively placed within clearly delineated categories, people are expected to conform to the expectations that characterise the social slot that they occupy. Many of the criticisms of identification schemes implicitly address these discursive practices, for example, through descriptions like 'citizen', 'immigrant' and 'asylum seeker'. Additional concerns emerge from the discursive practices applied to individuals who don't fit mainstream classifications. These include transgendered individuals who are neither 'male' nor 'female' and those with 'chaotic' lifestyles such as the homeless with no fixed abode.

Tyworth's paper shifts the focus from individual identity to organisational identity. He studied two integrated justice information systems that serve law enforcement activities in two locations in the United States, the San

Diego Metro Area California and the Commonwealth of Pennsylvania. The paper draws on a theory of organisational identity that differentiates between ideational (internal perception of what the organisation is), definitional (specific features that make the organisation unique) and phenomenological (the identity as instantiated through its discourses and practices) aspects of organisational identity. The claim being examined is that differing organisational identities will serve as referents for the development of different kinds of systems even though they are serving similar kinds of customers. One of the organisations sees itself as being a centre for regional collaboration and hence does not impose its will on the other organisations it interacts with, the second case study site sees itself as an information broker and facilitator of access to justice related information. Thus although the two organisations appear to be fulfilling the same function, their differing identities result in different design and governance processes and hence resulting systems. For example, the 'centre for regional collaboration' consolidated the systems from within its network and was able to offer 'global query' of all data held in its repositories through a single front end whereas one of the consequences of 'information broker' was that its system design meant that it was unable to offer this kind of functionality.

Identification mechanisms are needed to control who has access to the sensitive data about gangs, criminal convictions etc. held on the justice systems studied by Tyworth. Assessing the weakness of such identification systems is a key task of any risk assessment for a critical piece of technology infrastructure. However, as Tyworth's study demonstrates, the particular form that the justice system takes is not based on technological considerations alone but is also shaped by the organisational identity of its host. Information systems researchers therefore need to adapt existing security assessment methods to include consideration of organisational identity including the implications of this concept for proposed risk mitigation strategies.

The final paper, by Schultze, shifts to cyberspace, in particular Second Life. The paper studies a number of Second Life entrepreneurs to understand how embodied identity is performed in virtual worlds. The study explicitly differentiates between disembodied, representational and performative perspectives on identity performance in virtual worlds. Drawing on data collected from nine Second Life entrepreneurs who ran in-world business, Schultze explores the game-like nature of much Second Life interaction and the strategies entrepreneurs used to enact their identity. In particular she focuses on the entrepreneurs' performance of personhood and individuality in order to establish themselves as authentic people and reliable business partners.

While information systems researchers have explored many of the assumptions about identification and trust that shape transactions, for example with real-world entrepreneurs or e-commerce websites, this study demonstrates how Second Life entrepreneurs use a variety of identity and identification mechanisms to replicate these processes online. Better understanding of their effectiveness online can also enhance our understanding of their offline equivalents. As this review and the selected papers have demonstrated, information systems researchers have much to contribute to the study of identity and identification. In addition, by considering the close interplay between the two concepts, further innovative research challenges emerge that draw on key elements of both areas.

Acknowledgements

An earlier version of the review of identity research appeared as Gal & Kjaergaard (2009). The authors are very grateful for the advice and support of the *EJIS* editors in preparing this editorial. Thanks are also due to the *EJIS* office for their assistance in managing the review process. Financial support for the special issue workshop in Helsinki was provided by the LSE Staff Research Fund.

About the authors

Edgar A. Whitley is a Reader in Information Systems in the Department of Management at the London School of Economics and Political Science. Edgar was the research coordinator of the influential LSE Identity Project on the U.K.'s proposals to introduce biometric identity cards; proposals that were scrapped following the 2010 General Election. His book with Gus Hosein *Global Challenges for Identity Policies* was published by Palgrave in 2010. Edgar has also advised governments in Brazil, Chile, Ecuador and Jamaica about the political, technological and social challenges of effective identity policies. Edgar has a B.Sc. (Econ) and Ph.D. in Information Systems, both from the LSE. He is the co-editor of Information Technology and People and has served as conference chair for the European Conference on Information Systems, track chair for the International Conference on Information Systems and was an associate editor for the *European Journal of Information Systems* and *MIS Quarterly*. In addition to his research on privacy and identity, Edgar is also researching cloud computing and is the co-author of book *Moving to the Cloud Corporation*, published by Palgrave 2014.

Uri Gal is a Senior Lecturer at the University of Sydney Business School. Before joining the University in 2010 he was an Assistant Professor of Information Systems at the Center for Applied Information and Communication Technology at Copenhagen Business School. He holds a Ph.D. degree in Information Systems from Case Western Reserve University and an M.Sc. degree in Organisational Psychology from the London School of Economics and Political Science. His research takes a social view of organisational processes in the context of the implementation and use of

information systems. He is particularly interested in the relationships between people and technology in organisations and the changes in the nature of work practices, organisational identities, and interactions associated with the introduction of new information technologies.

Annemette Kjaergaard is an Associate Professor at the Copenhagen Business School. She holds a Ph.D. degree in Business Economics and Information Systems from Copenhagen Business School and an M.Sc. degree in Computer Science and English from Roskilde University in Denmark. Her research interests are organisational and human implications of implementation and use of information systems with a particular focus on social and organisational identity as well as on organisational change processes.

References

AICHHOLZER G and STRAUSS S (2010) Electronic identity management in e-government 2.0: exploring a system innovation exemplified by Austria. *Information Polity* **15**(**1**/**2**), 139–152.

ALBERT S, ASHFORTH BE and DUTTON JE (2000) Organizational identity and identification: charting new waters and building new bridges. *Academy of Management Review* **25**(**1**), 13–17.

ALBERT S and WHETTEN DA (1985) Organizational identity. In *Research in Organizational Behavior* (CUMMINGS LL and STAW BM, Eds), pp 263–295, JAI Press, Greenwich, CT.

AllAfrica.com. (2010) Mozambique: Biometric passports rejected. (22 March) [WWW document] http://allafrica.com/stories/201003221610.html (accessed 18 October 2013).

ALTERMAN A (2003) 'A piece of yourself': ethical issues in biometric identification. *Ethics and Information Technology* **5**(**3**), 139–150.

ALVAREZ R (2008) Examining technology, structure and identity during an enterprise system implementation. *Information Systems Journal* **18**(**2**), 203–224.

ALVESSON M (1994) Talking in organizations: managing identity and impressions in an advertising agency. *Organization Studies* **15**(**4**), 535–563.

ALVESSON M, ASHCRAFT KL and THOMAS R (2008) Identity matters: reflections on the construction of identity scholarship in organization studies. *Organization* **15**(**1**), 5–28.

AMOORE L (2008) Governing by identity. In *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (BENNETT CJ and LYON D, Eds), pp 21–36, Routledge, London.

ARORA S (2008) National e-ID card schemes: a European overview. *Information Security Technical Report* **13**(**2**), 46–53.

ASHFORTH BE and MAEL F (1989) Social identity theory and the organization. *Academy of Management Review* **14**(**1**), 20–39.

ASHFORTH BE and MAEL F (1996) Organizational identity and strategy as a context for the individual. In *Advances in Strategic Management* (BAUM JAC and DUTTON JE, Eds), pp 19–64, JAI Press, Greenwich, CT.

ATKESON LR, BRYANT LA, HALL TE, SAUNDERS KL and ALVAREZ RM (2010) A new barrier to participation: heterogeneous application of voter identification policies. *Electoral Studies* **29**(**1**), 66–73.

BACKHOUSE J, HSU C, TSENG JC and BAPTISTA J (2005) A question of trust: an economic perspective on quality standards in the certification services market. *Communications of the ACM* **48**(**9**), 87–91.

BAI X, NUNEZ M and KALAGNANAM JR (2012) Managing data quality risk in accounting information systems. *Information Systems Research* **23**(**2**), 453–473.

BAILEY SGM and CAIDI N (2005) How much is too little? Privacy and smart cards in Hong Kong and Ontario. *Journal of Information Science* **31**(**5**), 354–364.

BALL K, DANIEL EM and STRIDE C (2012) Dimensions of employee privacy: an empirical study. *Information Technology and People* **25**(**4**), 376–394.

BARNARD-WILLS D and ASHENDEN D (2011) Public sector engagement with online identity management. *Identity in the Information Society* **3**(**1**), 657–674.

BARRETT MI and SCOTT SV (2004) Electronic trading and the process of globalization in traditional futures exchanges: a temporal perspective. *European Journal of Information Systems* **13**(**1**), 65–79.

BARRETT MI and WALSHAM G (1999) Electronic trading and work transformation in the London insurance market. *Information Systems Research* **10**(**1**), 1–22.

BBC NEWS. (2013) Bomb threat tweet sent to classicist Mary Beard. (4 August) [WWW document] http://www.bbc.co.uk/news/23565145 (accessed 18 October 2013).

BEECH N and HUXHAM C (2004) Cycles of identity formation in interorganizational collaborations. *International Studies of Management & Organization* **33**(**3**), 28–52.

BENNETT CJ and LYON D (Eds) (2008) *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. Routledge, London.

BERGHEL H (2000) Identity theft, social security numbers and the web. *Communications of the ACM* **43**(**2**), 17–21.

BERGHEL H (2006) Fungible credentials and next-generation fraud. *Communications of the ACM* **49**(**12**), 15–19.

BERNAT L (2011) National strategies and policies for digital identity management in OECD countries. *OECD* [WWW document] http://dx.doi.org/10.1787/5kgdzvn5rfs2-en (accessed 18 October 2013).

BEYNON-DAVIES P (2011) The U.K. national identity card. *Journal of Information Technology Teaching Cases* **1**(**1**), 12–21.

BING J (2009) Protecting personal data in wartime: the destruction of the alphabetic tabulators in Oslo. *Computer Law & Security Review* **25**(**1**), 89–96.

BIRCH DGW (2009) Psychic ID: a blueprint for a modern national identity scheme. *Identity in the Information Society* **1**(**1**), 189–201.

BOSE I, NGAI EWT, TEO TSH and SPIEKERMANN S (2009) Managing RFID projects in organizations. *European Journal of Information Systems* **18**(**6**), 534–540.

BOWYER KW, BAKER SE, HENTZ A, HOLLINGSWORTH K, PETERS T and FLYNN PJ (2009) Factors that degrade the match distribution in iris biometrics. *Identity in the Information Society* **2**(**3**), 327–343.

BROEDERS D (2007) The new digital borders of Europe: EU databases and the surveillance of irregular migrants. *International Sociology* **22**(**1**), 71–92.

BROMBY M (2010) Identification, trust and privacy: how biometrics can aid certification of digital signatures. *International Review of Law Computers & Technology* **24**(**1**), 133–141.

Cabinet Office. (2012) GPG 43 Requirements for secure delivery of online public services. (version 1.1) (December) [WWW document] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/138004/GPG_43_RSDOPS_issue_1.1_Dec-2012.pdf (accessed 18 October 2013).

Cabinet Office. (2013a) Draft Identity Assurance Principles. (17 June) [WWW document] https://www.gov.uk/government/consultations/draft-identity-assurance-principles (accessed 18 October 2013).

Cabinet Office. (2013b) GPG 45 Identity proofing and verification of an individual. (Version 2.0) (May) [WWW document] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204448/GPG_45_Identity_proofing_and_verification_of_an_individual_2.0_May-2013.pdf (accessed 18 October 2013).

CAMERON K (2005) The laws of identity. (5 November) [WWW document] http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (accessed 18 October 2013).

CARTER B (1998) Implementation implications of biometrics. *Information Security Technical Report* **3**(**1**), 60–69.

CHENEY G and CHRISTENSEN LT (2001) Organizational identity: linkages between 'internal' and 'external' organizational communication. In *The New Handbook of Organizational Communication* (JABLIN FM and PUTNAM LL, Eds), pp 231–269, Sage, Thousand Oaks.

CIBORRA C and ASSOCIATES. (2000) *From Control to Drift: The Dynamics of Corporate Information Infrastructures*. Oxford University Press, Oxford.

COLLINGS T (2008) Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID). *Information Security Technical Report* **13**(**2**), 61–70.

COMPEAU D, MARCOLIN B, KELLEY H and HIGGINS C (2012) Research commentary – generalizability of information systems research using student subjects – a reflection on our practices and recommendations for future research. *Information Systems Research* **23**(**4**), 1093–1109.

CORDELLA A and WILLCOCKS LP (2010) Outsourcing, bureaucracy and public value: reappraising the notion of the 'contract state'. *Government Information Quarterly* **27**(**1**), 82–88.

CORLEY KG and GIOIA DA (2003) Semantic learning as change enabler: relating organizational identity & organizational learning. In *Handbook of Organizational Learning and Knowledge Management* (EASTERBY-SMITH M and LYLES MA, Eds), pp 621–636, Blackwell, London.

CORLEY KG and GIOIA DA (2004) Identity ambiguity and change in the wake of a corporate spin-off. *Administrative Science Quarterly* **49**(**2**), 173–208.

CORLEY KG, HARQUAIL CV, PRATT MG, GLYNN M, FIOL CM and HATCH MJ (2006) Guiding organizational identity through aged adolescence. *Journal of Management Inquiry* **15**(**2**), 85–99.

CORNELISSEN JP, HASLAM SA and BALMER JMT (2007) Social identity, organizational identity and corporate identity: towards an integrated understanding of processes, patternings and products. *British Journal of Management* **18**(**special issue**), 1–16.

CURRAH P and MULQUEEN T (2011) Securitizing gender: identity, biometrics and transgender bodies at the airport. *Social Research* **78**(**2**), 557–582.

DARKING ML and WHITLEY EA (2007) Towards an understanding of FLOSS: infrastructures, materiality and the digital business ecosystem. *Science & Technology Studies* **20**(**2**), 13–33.

DAUGMAN J (1998) Recognizing people by their iris patterns. *Information Security Technical Report* **3**(**1**), 33–39.

DAVIES SG (1998) Biometrics: a civil liberties and privacy perspective. *Information Security Technical Report* **3**(**1**), 90–94.

DAVIS CJ and HUFNAGEL EM (2007) Through the eyes of experts: a socio-cognitive perspective on the automation of fingerprint work. *MIS Quarterly* **31**(**4**), 681–704.

DAVIS FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly* **13**(**3**), 319–340.

DAVIS FD, BAGOZZI RP and WARSHAW PR (1989) User acceptance of computer technology: a comparison of two theoretical models. *Management Science* **35**(**8**), 982–1003.

DE COCK D, SIMOENS K and PRENEEL B (2008) Insights on identity documents based on the Belgian case study. *Information Security Technical Report* **13**(**2**), 54–60.

DICKEY MH, BURNETT G, CHUDOBA KM and KAZMER MM (2007) Do you read me? Perspective making and perspective taking in chat communities. *Journal of the AIS* **8**(**1, Article 3**), 47–70.

DINEV T, HART P and MULLEN MR (2008) Internet privacy concerns and beliefs about government surveillance – an empirical investigation. *Journal of Strategic Information Systems* **17**(**3**), 214–233.

DOOLIN B (2002) Enterprise discourse, professional identity and the organizational control of hospital clinicians. *Organization Studies* **23**(**4**), 369–390.

DOOLIN B (2003) Narratives of change: discourse, technology and organization. *Organization Studies* **10**(**4**), 751–770.

DUNLEAVY P (2005) Written evidence to the Public Administration Select Committee. (24 November) [WWW document] http://www2.lse.ac.uk/ERD/pressAndInformationOffice/PDF/IDCard_Nov05WrittenEvidence.pdf (accessed 18 October 2013).

DUNLEAVY P, MARGETTS H, BASTOW S and TINKLER J (2006) *Digital Era Governance: IT Corporations, the State and E-Government*. Oxford University Press, Oxford.

DUTTON JE (1997) Strategic agenda building in organizations. In *Organisational Decision Making* (SHAPIRA Z, Ed), Cambridge University Press, Cambridge.

DUTTON JE and DUKERICH JM (1991) Keeping an eye on the mirror: image and identity in organizational adaptation. *Academy of Management Journal* **34**(**3**), 517–554.

DUTTON JE, DUKERICH JM and HARQUAIL CV (1994) Organizational images and member identification. *Administrative Science Quarterly* **39**(**2**), 239–263.

ENISA. (2009) Privacy Features of European eID Card Specifications. (27 January) [WWW document] http://www.enisa.europa.eu/activities/identity-and-trust/trust-services/eid-cards-en (accessed 18 October 2013).

ERIKSSON O and AGERFALK P (2010) Rethinking the meaning of identifiers in information infrastructures. *Journal of the Association for Information Systems* **11**(**8**), 433–454.

Estonia Digi – ID. (2013) Digi-ID. [WWW document] http://www.politsei.ee/en/teenused/isikut-toendavad-dokumendid/digi-id/ (accessed 18 October 2013).

European Parliament. (2012) Fighting cyber crime and protecting privacy in the cloud. Directorate General for Internal Policies; Policy Department C: Citizens' rights and constitutional affairs. (October) [WWW document] http://www.europarl.europa.eu/committees/en/studies download.html?languageDocument=EN&file=79050 (accessed 18 October 2013).

FAYARD A and DESANCTIS G (2010) Enacting language games: the development of a sense of we-ness in online forums. *Information Systems Journal* **20**(**4**), 383–416.

FIOL CM (1991) Managing culture as a competitive resource: an identity-based view of sustainable competitive. *Journal of Management* **17**(**1**), 191–211.

FIOL CM (2002) Capitalizing on paradox: the role of language in transforming organizational identities. *Organization Science* **13**(**6**), 653–666.

FIPR. (2009) Database state: a report commissioned by the Joseph Rowntree Reform Trust Ltd. (22 March) [WWW document] http://www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf (accessed 18 October 2013).

FORMAN C, GHOSE A and WIESENFELD B (2008) Examining the relationship between reviews and sales: the role of social information in electronic markets. *Information Systems Research* **19**(**3**), 291–313.

FROOMKIN AM (2009) Identity cards and identity romanticism. In *Lessons From the Identity Trail: Anonymity, Privacy and Identity in A Networked Society* (KERR I, Ed), pp 245–263, Oxford University Press, Oxford.

GAL U and KJAERGAARD A (2009) Identity in information systems. In *17th European Conference on Information Systems* (Newell S, Whitley EA, Wareham NPJ and Mathiassen L, Eds), pp 1999–2011, Verona, Italy. [WWW document] http://is2.lse.ac.uk/asp/aspecis/20090166.pdf (accessed 18 October 2013).

GAL U, LYYTINEN K and YOO Y (2008) The dynamics of it boundary objects, information infrastructures, and organizational identities: the introduction of 3D modelling technologies into the architecture, engineering, and construction industry. *European Journal of Information Systems* **17**(**3**), 290–304.

GARFINKEL SL (1995) Risks of social security numbers. *Communications of the ACM* **38**(**10**), 146.

GATES K (2008) The United States Real ID Act and the securitization of identity. In *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (BENNETT CJ and LYON D, Eds), pp 218–232, Routledge, London.

GATES KA (2005) Technologies of identity and the identity of technology: race and the social construction of biometrics. In *Race, Identity and Representation in Education* (MCGARTHY C and CRICHLOW W, Eds), pp 59–71, Routledge, New York.

GIOIA DA (1998) From individual to organizational identity. In *Identity in Organizations – Building Theory Through Conversations* (WHETTEN DA and GODFREY PC, Eds), pp 17–31, Sage, Thousand Oaks, CA.

GIOIA DA and CHITTIPEDDI K (1991) Sensemaking and sensegiving in strategic change initiation. *Strategic Management Journal* **12**(**6**), 433–448.

GIOIA DA, SCHULTZ M and CORLEY KG (2000) Organizational identity, image, and adaptive instability. *Academy of Management Review* **25**(**1**), 63–81.

GIOIA DA and THOMAS JB (1996) Identity, image, and issue interpretation: sensemaking during strategic change in academia. *Administrative Science Quarterly* **41**(**3**), 370–403.

HAGGERTY K and GAZSO A (2005) The public politics of opinion research on surveillance and privacy. *Surveillance and Society* **3**(**2/3**), 173–180.

HALPERIN R and BACKHOUSE J (2008) A roadmap for research on identity in the information society. *Identity in the Information Society* **1**(**1**), 71–87.

HARBITZ M and BOEKLE-GIUFFRIDA B (2009) Democratic governance, citizenship, and legal identity: linking theoretical discussion and operational reality. InterAmerican Development Bank. [WWW document] http://www.iadb.org/intal/intalcdi/PE/2009/03791.pdf (accessed 18 October 2013).

HARBITZ M and MOLINA JCB (2010) Civil registration and identification glossary. InterAmerican Development Bank. [WWW document] http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=35308547 (accessed 18 October 2013).

HASLAM SA (2001) *Psychology in Organizations: The Social Identity Approach*. Sage, London.

HASLAM SA and ELLEMERS N (2005) Social identity in industrial and organizational psychology: concepts, controversies and contributions. In *International Review of Industrial and Organizational Psychology* (HODGKINSON GP and FORD JK, Eds), pp 39–118, John Wiley & Sons Ltd, Chichester.

HENFRIDSSON O and BYGSTAD B (2013) The generative mechanisms of digital infrastructure evolution. *MIS Quarterly* **37**(**3**), 896–931.

HM Passport Office. (2011) Basic passport checks. (9 February) [WWW document] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118783/basic-passport-checks.pdf (accessed 18 October 2013).

HOIKKANEN A, BACIGALUPO M, COMPAÑÓ R, LUSOLI W and MAGHIROS I (2010) New challenges and possible policy options for the regulation of electronic identity. *Journal of International Commercial Law and Technology* **5**(**1**), 1–10.

Home Affairs Committee. (2008) A surveillance society? (8 June) [WWW document] http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf (accessed 18 October 2013).

HORNUNG G (2005) Biometric passports and identity cards: technical, legal and policy issues. *European Public Law* **11**(**4**), 501–514.

HORNUNG G and SCHNABEL C (2009) Data protection in Germany I: the population census decision and the right to informational self-determination. *Computer Law & Security Review* **25**(**1**), 84–88.

IAS Project. (2011) Study on an electronic identification, authentication and signature policy. [WWW document] http://www.iasproject.eu/ (accessed 18 October 2013).

ICAO. (2003) Technical advisory group on machine readable travel documents. Fourteenth meeting International Civil Aviation Organisation. (6–9 May) [WWW document] http://www2.icao.int/en/MRTD/Downloads/TAG-MRTD%20Reports/TAG-MRTD_14%20Report.pdf (accessed 18 October 2013).

INTRONA LD and NUSSENBAUM H (2009) Facial recognition technology: a survey of policy and implementation issues. (April) [WWW document] http://www.nyu.edu/projects/nissenbaum/papers/facial_recognition_report.pdf (accessed 18 October 2013).

JAHNG JJ, JAIN H and RAMAMURTHY K (2002) Personality traits and effectiveness of presentation of product information in e-business systems. *European Journal of Information Systems* **11**(**3**), 181–195.

JAIN AK (2007) Biometric recognition: Q&A. *Nature* **449**(**September**), 38–40.

JAIN AK, ROSS A and PRABHAKAR S (2004) An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics* **14**(**1**), 4–20.

JUNG CG (1971) *Collected Works, Volume Six: Psychological Types*. Princeton University Press, Princeton, NJ.

KABATOFF M and DAUGMAN J (2008) Pattern recognition: biometrics, identity and the state – an interview with john daugman. *Biosocieties* **3**(**1**), 81–86.

KALLINIKOS J (2004) Deconstructing information packages: organizational and behavioural implications of erp systems. *Information Technology & People* **17**(**1**), 8–30.

KERR I, STEEVES V and LUCOCK C (Eds) (2009) *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. Oxford University Press, Oxford.

KIESER A and LEINER L (2009) Why the rigour – relevance gap in management research is unbridgeable. *Journal of Management Studies* **46**(**3**), 516–533.

KIM H, CHAN H and ATREYI K (2012) What motivates people to purchase digital items on virtual community websites? The desire for online self-presentation. *Information Systems Research* **23**(**4**), 1232–1245.

KOOPS B-J, LEENES R, MEINTS M, NVD MEULEN and JAQUET-CHIFFELLE D-O (2009) A typology of identity-related crime: conceptual, technical, and legal issues. *Information, Communication & Society* **12**(**1**), 1–24.

KRAKOVSKY M (2011) India's elephantine effort. *Communications of the ACM* **54**(**1**), 23–24.

LAMB R and DAVIDSON E (2005) Information and communication technology challenges to scientific professional identity. *The Information Society* **21**(**1**), 1–24.

LI C, PETERS GF, RICHARDSON VJ and WATSON MW (2012) The consequences of information technology control weaknesses on management information systems: the case of sarbanes–oxley internal control reports. *MIS Quarterly* **36**(**1**), 179–203.

LI X, HESS TJ and VALACICH JS (2008) Why do we trust new technology? A study of initial trust formation with organizational information systems. *Journal of Strategic Information Systems* **17**(**1**), 39–71.

LIM SS, CHO H and SANCHEZ MR (2009) Online privacy, government surveillance and national ID cards. *Communications of the ACM* **52**(**12**), 116–120.

LIPS AMB, TAYLOR JA and ORGAN J (2009) Identity management, administrative sorting and citizenship in new modes of government. *Information, Communication & Society* **12**(**5**), 715–734.

LIPS M (2013) Reconstructing, attributing and fixating citizen identities in digital-era government. *Media, Culture and Society* **35**(**1**), 61–70.

LYON D (2007) *Surveillance Studies: An Overview*. Polity, Cambridge.

LYON D (2009) *Identifying Citizens: ID Cards as Surveillance*. Polity, Cambridge.

MA M and AGARWAL R (2007) Through a glass darkly: information technology design, identity verification, and knowledge contribution in online communities. *Information Systems Research* **18**(**1**), 42–67.

MAGNET SA (2011) *When Biometrics Fail: Gender, Race and the Technology of Identity*. Duke University Press, Durham.

MAHLER T (2013) Governance models for interoperable electronic identities. *Journal of International Commercial Law and Technology* **8**(**2**), 148–159.

MARTIN AK and ANDRADE NNGD (2013) Friending the taxman: on the use of social networking services for government eID in Europe. *Telecommunications Policy* **37**(**9**), 715–724.

MARTIN AK and WHITLEY EA (2013) Fixing identity? Biometrics and the tensions of material practices. *Media, Culture and Society* **35**(**1**), 52–60.

MONTEIRO E and HANSETH O (1995) Social shaping of information infrastructure: on being specific about the technology. In *Information technology and changes in organizational work* (ORLIKOWSKI WJ, WALSHAM G, JONES MR and DEGROSS JI, Eds), pp 325–343, Chapman & Hall, London.

MOORE GC and BENBASAT I (1991) Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research* **2**(**3**), 192–220.

MORDINI E and MASSARI S (2008) Body, biometrics and identity. *Bioethics* **27**(**9**), 488–498.

MURAKAMI WOOD D and FRIMINO R (2009) Empowerment or represssion? Opening up questions of identification and surveillance in Brazil through a case of 'identity fraud'. *Identity in the Information Society* **2**(**3**), 297–317.

NAG R, CORLEY KG and GIOIA DA (2007) The intersection of organizational identity,knowledge, and practice: attempting strategic change via knowledge grafting. *Academy of Management Journal* **50**(**4**), 821–847.

NEYLAND D (2009) Who's who? The biometric future and the politics of identity. *European Journal of Criminology* **6**(**2**), 135–155.

NG-KRUELLE G, SWATMAN PA, HAMPE JF and REBNE DS (2006) Biometrics and e-identity (e-passport) in the European Union: end-user perspectives on the adoption of a controversial innovation. *Journal of Theoretical and Applied Electronic Commerce Research* **1**(**2**), 12–35.

OLLIER-MALA TERRE A, ROTHBARD N and BERG J (2013) When worlds collide in cyberspace: how boundary work in online social networks impacts professional relationships. *Academy of Management Review* **38**(**4**), 645–669.

ORIHUELA L (2009) Peruvian national registry of identification and civil states: a successful study in e-governance. *I-ways Journal of E-Government Policy and Regulation* **32**(**2**), 99–103.

OTJACQUES B, HITZELBERGER P and FELTZ F (2007) Interoperability of E-government information systems: issues of identification and data sharing. *Journal of Management Information Systems* **23**(**4**), 29–52.

Perri 6. (2005) Should we be compelled to have identity cards? Justifications for the legal enforcement of obligations. *Political Studies* **53**(**2**), 243–261.

POLLOCK N and WILLIAMS R (2009) The sociology of a market analysis tool: how industry analysts sort vendors and organize markets. *Information and Organization* **19**(**2**), 129–151.

PRATT MG and FOREMAN PO (2000) Classifying managerial responses to multiple organizational identities. *Academy of Management Review* **25**(**1**), 18–42.

RAHAMAN A and SASSE MA (2010) A framework for the lived experience of identity. *Identity in the Information Society* **3**(**3**), 605–638.
RAMAKUMAR R (2010) The unique ID project in India: a skeptical note. In *ICEB 2010, Lecture Notes in Computer Science 6005* (KUMAR A and ZHANG D, Eds), pp 153–167, Springer, Berlin.
RAVASI D and SCHULTZ M (2006) Responding to organizational identity threats: exploring the role of organizational culture. *Academy of Management Journal* **49**(**3**), 433–458.
REHMAN-GREENE M (1998) Security considerations in the use of biometric devices. *Information Security Technical Report* **3**(**1**), 77–80.
ROMERO JJ (2012) India's big bet on identity. *IEEE Spectrum* **49**(**3**), 48–56.
ROTENBERG M (2006) Real ID, Real trouble? *Communications of the ACM* **49**(**3**), 128–128.
SADIQ K (2009) *Paper Citizens: How Illegal Immigrants Acquire Citizenship in Developing Countries*. Oxford University Press, Oxford.
SARKER S and SAHAY S (2003) Understanding virtual team development: an interpretive study. *Journal of the AIS* **4**(**1**, **Article 1**), 1–38.
SASS JS and CANARAY DJ (1991) Organizational commitment and identification: an examination of conceptual and operational convergence. *Western Journal of Speech Communication* **55**(**3**), 275–293.
SCHULTZ M, HATCH MJ and LARSEN MH (2000) *The Expressive Organization: Linking Identity, Reputation, and the Corporate Brand*. Oxford University Press, Oxford.
SCHWARTZ A (2011) Identity management and privacy: a rare opportunity to get it right. *Communications of the ACM* **54**(**6**), 22–24.
SCOTT SV and ORLIKOWSKI WJ (2012) Reconfiguring relations of accountability: materialization of social media in the travel sector. *Accounting, Organizations and Society* **37**(**1**), 26–40.
SELTSIKAS P and O'KEEFE RM (2010) Expectations and outcomes in electronic identity management: the role of trust and public value. *European Journal of Information Systems* **19**(**1**), 93–103.
SHAIKH SA and RABAIOTTI JR (2010) Characteristic trade-offs in designing large-scale biometric-based identity management systems. *Journal of Network and Computer Applications* **33**(**3**), 342–351.
Sir James Crosby. (2008) Challenges and opportunities in identity assurance. (6 March) [WWW document] http://www.statewatch.org/news/2008/mar/uk-nat-identity-crosby-report.pdf (accessed 18 October 2013).
SLUSS DM and ASHFORTH BE (2007) Relational identity and identification: defining ourselves through work relationships. *Academy of Management Review* **32**(**1**), 9–32.
SMITH HA and MCKEEN JD (2011) The identity management challenge. *Communications of the AIS* **28**(**Article 11**), 169–178.
SPROKKEREEF A and DE HERT P (2007) Ethical practice in the use of biometric identifiers within the EU. *Law, Science and Policy* **3**(**2**), 177–202.
STAR SL and RUHLEDER K (1996) Steps toward an ecology of infrastructure: design and access for large information space. *Information Systems Research* **7**(**1**), 111–134.
TAJFEL H and TURNER JC (1979) An integrative theory of intergroup conflict. In *The Social Psychology of Intergroup Relations* (AUSTIN WG and WORCHEL S, Eds), pp 33–47, Brooks/Cole, Monterey, CA.
TENE O (2013) Me, Myself and I: aggregated and disaggregated identities on social networking services. *Journal of International Commercial Law and Technology* **8**(**2**), 118–133.
The Tribune. (2012) Coriander, s/o Pulav, gets Aadhaar card in Andhra. (16 April) [WWW document] http://www.tribuneindia.com/2012/20120416/main6.htm (accessed 18 October 2013).
THOMAS R (2005) Biometrics, international migrants and human rights. *European Journal of Migration Law* **7**(**4**), 377–411.
TURKLE S (1996) *Life on the Screen: Identity in the Age of the Internet*. Weidenfeld & Nicholson, London.
TURNER JC (2005) Explaining the nature of power: a three-process theory. *European Journal of Social Psychology* **35**(**1**), 1–22.
UNICEF. (2007) Progress for Children: A World Fit for Children Statistical Review, Number 6. *United Nations Children's Fund*. [WWW document] http://www.unicef.org/publications/files/Progress_for_Children_No_6_revised.pdf (accessed 18 October 2013).
VAN AKKEREN J and ROWLANDS B (2007) An epidemic of pain in an Australian radiology practice. *European Journal of Information Systems* **16**(**6**), 695–711.
VAN ALSENOY B and DE COCK D (2008) Due processing of personal data in eGovernment? A case study of the Belgian electronic identity card. *Datenschutz und Datensicherheit* **32**(**3**), 178–183.
VAN DIJK J (2013) You have one identity: performing the self on facebook and LinkedIn. *Media, Culture and Society* **35**(**2**), 199–215.
WALSHAM G (1998) IT and changing professional identity: micro-studies and macro-theory. *Journal of the American Society for Information Science* **49**(**12**), 1081–1089.
WEICK KE (1995) *Sensemaking in Organizations*. Sage, Thousand Oaks, CA.
WEIGELT C (2013) Leveraging supplier capabilities: the role of locus of capability deployment. *Strategic Management Journal* **34**(**1**), 1–21.
WHITLEY EA (2013) On technology neutral policies for e-identity: a critical reflection based on U.K. identity policy. *Journal of International Commercial Law and Technology* **8**(**2**), 134–147.
WHITLEY EA and HOSEIN G (2010a) *Global Challenges for Identity Policies*. Palgrave Macmillan, Basingstoke.
WHITLEY EA and HOSEIN G (2010b) Global identity policies and technology: do we understand the question? *Global Policy* **1**(**2**), 209–215.
WHITLEY EA and HOSEIN IR (2008a) Departmental influences on policy design: how the U.K. is confusing identity fraud with other policy agendas. *Communications of the ACM* **51**(**5**), 98–100.
WHITLEY EA and HOSEIN IR (2008b) Doing the politics of technological decision making: due process and the debate about identity cards in the U.K. *European Journal of Information Systems* **17**(**6**), 668–677.
WICKINS J (2007) The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification. *Science and Engineering Ethics* **13**(**1**), 45–54.
WILLCOCKS LP, REYNOLDS P and FEENY D (2007) Evolving IS capabilities to leverage the external IT services market. *MISQExecutive* **6**(**3**), 128–145.
WU J and LEDERER A (2009) A meta-analysis of the role of environment-based voluntariness in information technology acceptance. *MIS Quarterly* **33**(**2**), 419–432.
YUQING R *et al* (2012) Building members' attachment in online communities: applying theories of group identity and interpersonal bonds. *MIS Quarterly* **36**(**3**), 841–864.
ZUBOFF S (1988) *In the Age of the Smart Machine: The Future of Work and Power*. Basic Books, New York.