IDIS (2008) 1:71–87
DOI 10.1007/s12394-008-0004-0

# A roadmap for research on identity in the information society

## Identity in the information society journal volume 1 (1) paper no. 1

**Ruth Halperin · James Backhouse**

Received: 28 December 2007 / Accepted: 28 July 2008 / Published online: 20 December 2008


**Abstract** As research into identity in the information society gets into its stride, with contributions from many scholarly disciplines such as technology, social sciences, the humanities and the law, a moment of intellectual stocktaking seems appropriate. This article seeks to provide a roadmap of research currently undertaken in the field of identity and identity management showing how the area is developing and how disparate contributions relate to each other. Five different perspectives are proposed through which work in the identity field can be seen: tensions, themes, application areas, research focus and disciplinary approaches and taken together they provide a comprehensive overview of the intellectual territory currently being tilled by academia on this subject. This attempt at a coherent overview is offered in the spirit of debate and discussion, and the authors invite criticism, development and improvement. Another purpose of this paper is to provide an introduction to the range and type of research that the new journal *Identity in the Information Society* will publish, giving researchers working in the field a clearer idea of the scope of multidisciplinary study that is envisaged.

**Keywords** Identity in the information society · Roadmap of identity research · Multidisciplinary research · Digital identity · Privacy · Security

## Introduction

Identity in the information society is an emerging field in academic research and the consolidation is just beginning of the discussion of what constitutes digital identity.

R. Halperin · J. Backhouse (✉)
Information Systems and Innovation Group, Department of Management,
London School of Economics and Political Science, Houghton Street, London WC2A 2AE, UK
e-mail: James.Backhouse@lse.ac.uk

R. Halperin
e-mail: R.Halperin@lse.ac.uk

The unrelenting drive towards an Information Society has intensified a central problematic of the identity domain. The past years have witnessed an increasingly sophisticated use of personal information exploiting information and communication technology (ICT) to deliver a variety of services, and to drive and achieve different goals. This intensification has surfaced some of the pitfalls awaiting a brave new digitised future, and led to research into the multifaceted phenomenon of identity and its emerging forms. In this opening article of the new journal *Identity in the Information Society* we propose a roadmap that offers a basis for intellectual stocktaking as well as for reflecting on where future research might lead in this important topic of identity. As is the way with still-developing areas, and particularly one as contemporary as identity, any rigid boundaries may be soon inappropriate. Technological, political and commercial developments are constantly in ferment and offer new challenges to those seeking to impose intellectual order on a subject that is expanding (Galliers 2003). For example, in recent times we have seen in the UK a sharply contested debate around ID cards[1] that has raised the profile of identity issues far beyond any previous expectation, although the same questions that excite passions in UK cause scarcely a ripple on the surface of the body politic in many other European countries where identity cards are non-controversial (Backhouse and Halperin 2007).

A key aim of this paper is to locate existing research within its conceptual space, showing the relationships between ostensibly divergent threads and to identify where gaps may be forming. Research in identity has so far evolved in a piecemeal and even haphazard fashion, and technology and politics has driven the agenda. This is an attempt to map some of the intellectual terrain.

The Identity in the Information Society Journal was founded from the work of the FIDIS research project funded by the EU[2]. Founding a journal was one of the initial aims of this multidisciplinary research network and it is pleasing to see that aim being realized here. Naturally we draw on the FIDIS opus for many of our examples although realizing that there is both global interest and a worldwide community of researchers on this topic.

We develop the research roadmap on identity from five different perspectives, which while at times perhaps may overlap, we hope can still offer useful distinctive features. The first one is *Tensions*. It refers to major dilemmas and debates associated with identity in the information society, pointing to those contested territories whose hallmark consists of tension and contending interpretations. *Themes*, the second perspective of the research roadmap, explores emerging topics in the field of identity in the information society. Themes in this context represent preoccupations, or subjects that cut across boundaries, and we draw attention to three: conceptual foundations, identity management and identity systems and power structures. *Application Areas* is the third perspective, which emphasizes application domains that are relevant to studies of identity in the information society and thus the significance of sectoral analysis in the field of identity is highlighted. Increasing exploitation of identity information through deployment in ICT has penetrated more

[1] http://identityproject.lse.ac.uk/identityreport.pdf

[2] www.fidis.net

and more application areas with considerable effect. Government, Healthcare, Commerce more generally and the Finance sector are illustrative examples we refer to in this context. *Research Focus*, the fourth perspective, refers to current and future research foci on identity. Unlike tensions or themes, research foci operationalise specific concerns that are ripe for investigation, and thus, lead to results and research findings. They are also value indicators of what researchers deem to be worthwhile and feasible studies in the field. The research foci reveal the differing priorities relevant to studies of identity and indicate the kinds of studies undertaken and the type of results that are likely to be forthcoming. Finally, *Disciplinary approaches* is the last perspective in the agenda. It considers the relevance of different disciplinary standpoints, and the use of related theories, conceptual frameworks and models to inform research into identity in the information society. This category also addresses the interrelated subject of approaches to studies in identity, that result in some ambiguities regarding the nature of research in this area in terms of knowledge production processes and of epistemological underpinnings.

## Tensions in the identity discourse

The emerging discourse on digital identity reveals a number of key issues—major tensions and debates associated with identity in the information society. In what follows we point to those *contested territories* whose hallmark consists of contending interpretations. In circumscribing such ground, the main *problem areas* of identity in the information society are brought to the forefront, framed and marked as focal points for research.

### Security and privacy

The tensions that characterise the relations between security and privacy may be seen as the foremost issue in the discourse of identity in the information society. This issue has caught the eye of lobbyists, campaigners and researchers alike (Lessig 1999, p.154). Often, counterposing these two concepts suggests that they lie at either end of the same continuum, and hence more of one implies less of the other. For example, fighting crime and terrorism, deemed security (Etzioni 2002; Schneier 2006), has been offered as a plausible reason for breaching confidentiality, deemed privacy, and in the area of anti-money laundering and terrorist financing the old notions of bank secrecy have been considerably redefined.

However in these conflicts false dichotomies may be found: complying with data protection legislation means that maintaining personal information confidential cannot be achieved without "appropriate technical and organisational measures" (DPA 1998) in other words—appropriate security. Likewise, safeguarding the privacy of battered women who have sought refuge in a women's shelter directly contributes to their security. Security and privacy thus may sometimes not be opposed to each other but may indeed be mutually contributive. Cavoukian (2008) calls for a paradigm shift, from the zero-sum approach (security or privacy), to a positive-sum paradigm, whereby adding privacy measures to surveillance systems need not weaken security or functionality but rather, serve to enhance the overall

design. This approach of "radical pragmatism" involves the deployment of innovative privacy-enhancing "transformative" technologies, and is considered both desirable and feasible (Cavoukian 2008). The complex relationship between security and privacy however, gives rise to strong feelings, interesting questions and social implications and yet still contains much undiscovered terrain for researchers to explore (Royal Academy of Engineering 2007).

Interoperability

Another key tension, especially controversial in the context of identity management systems (IdMS), is that of interoperability. Interoperability here refers to the ability of using identity information from one identity management system in another (Backhouse 2006; Backhouse and Halperin 2008b). As such, interoperability may either expand or limit the benefits of identity management to citizens, businesses or governments. Amongst other issues (cf. Scholl 2005), the related tension between *risk and benefit* is heightened by the possibility of interoperable identity management systems. Here indeed are real dilemmas. On the one hand the citizen is only too aware of how annoying it is to be asked to supply time and again the same personal information to different departments of the same state: claiming one benefit often necessitates the same verification of identity that the citizen has already had to undergo when claiming another social benefit (Kinder 2003). Yet on the other hand, interoperable IdMS that involve large scale sharing of personal data among agencies raise considerable concerns for privacy and data protection (Six et al. 2005; Crossman 2007; Otjacques et al. 2007; Pounder 2008)

In her contribution to IDIS, Dowty (2008) critically analyses the potential risks of interoperable IdMS in the case of children databases. A growing number of databases in education, social care, health and youth justice store detailed information about children and facilitate its sharing between agencies. Some of this data is derived from in-depth personal assessment tools that are believed to 'predict' poor life outcomes such as criminality or social exclusion. These developments, however, create a new set of ethical and practical difficulties. The reduction in confidentiality brought about by routine inter-agency information sharing may deter children and their families from accessing services at all. Dowty points to the risk of habituating children to a very high level of surveillance, and to the possible effect of such widespread data-gathering on their safety and personal development.

Another area of significant complexity is joined-up eHealth systems. In eHealth, interoperability issues of identity, privacy and security are uppermost in the considerations of experts, citizens, and project managers alike (Anderson 2007). Sharing data between health care trusts will enable doctors in one part of the country to access data from another, when treatment is needed by for example a patient on holiday, away from home. At least, this is one reason given to justify the UK Electronic Care Record system, part of the Connecting for Health programme[3]. However, setting up a common spine for 60 million patient records requires that up to 400,000 health administrative staff would have access to personal medical

[3] http://www.connectingforhealth.nhs.uk/

information. How can privacy and data protection be ensured in such a situation? Similar issues arise in the case of the Swedish national electronic healthcare record, known as the National Patient Overview. HealthShare, the software to be implemented, is designed to enable the sharing of patient information between regional and local care providers in both the public and private sectors.[4] The question of whether to centralise or distribute identity management systems also arises—one approach is to emphasise the existing local control of such information and hence sharply define responsibilities, and liabilities, when personal data is made available outside the "home" system[5].

## Convenience and intrusiveness

A similar conflict, between convenience and intrusiveness, arises from technologies of identity. Many new technologies are emerging that exploit identity management techniques to offer new services to the public. Radio Frequency Identification (RFID), smart cards, automated profiling, biometric devices, mobile phones; all present great opportunities for service providers to enrich their market offerings and provide services and packages that attractively leverage the growing data shadow cast by digital consumption. RFID allows the identity management system to track the consumer from one retail experience to another so that the revealed patterns of expenditure ensure that one can be offered only certain kinds of marketed goods and services (Eckfeldt 2005). On the one hand this may be a unique opportunity to confound junk mailers, but on the other it may mean that an algorithm will decide what the consumer apparently wants and will be offered.

Another issue arises when mobile telephone service providers offered a tracking service to parents to track the movements of children through their logs of location data[6]. Needless to say, this service was taken up and used for many other kinds of privacy-intrusive tracking. So a related issue in this is that of *function creep*. Pounder (2008), in his contribution to this IDIS volume, goes further and deems function creep an inevitability to be coped with. Data collected for one purpose will very often, it seems, be used for another. In any case, law enforcement agencies will always demand access to any information, once collected, in the interests of fighting crime. Those who complain can be easily brushed aside as probably having something to hide.

Here we have sought to outline some of the major dilemmas and debates associated with identity in the information society. In the current discourse, security and privacy, interoperability and conflicts between convenience and intrusiveness are illustrative examples of such issues. The research community must be encouraged to study those issues that arouse debate and controversy in society. Such debates need to be valued as they are fundamental to the purpose of informing research directions and the decisions of funding councils and policy makers.

[4] http://www.e-health-insider.com/Features/item.cfm?&docId=261

[5] http://www.ehiprimarycare.com/news/3952/dh_group_to_look_at_wider_nhs_crs_access

[6] http://www.ericsson.com/solutions/operators/news/2006/q3/20060915_childtracking.shtml

## Themes for identity

Emerging themes in the field of identity and the information society call for exploration. Themes in this context represent more focused preoccupations, or sub-topics that cut across boundaries, but still lie within the broad area of identity. Here we will draw attention to three such themes that arose within FIDIS research, namely, identity fundamentals, identity management and identity systems and power structures. But these are not exhaustive and more are expected to emerge over time.

### Conceptual foundations of identity and e-identity

Establishing identity fundamentals, or the conceptual foundations of identity, is proposed as a research theme, referring to the task of defining the semantics of identity in the Information Society together with other identity-related concepts—how they are used, how they might be used and abused, how they ought to be defined in order to respect the fundamental rights of the citizen, how they can support identity systems that interoperate.

As more research on identity emerges, there is a need for clarity and agreement on definitions, distinctions and conceptualizations in order for the objects of study to be more clearly framed (Brubaker and Cooper 2000). Fundamental concepts in this area include, physical, digital, virtual, partial and cyber identity; derived identity; pseudonymity; anonymity; personalization and others. In this first volume of IDIS, Roger Clarke (2008) offers a much-needed set of working definitions of key terms that underpin studies of identity in the information society. They are offered not as authoritative interpretations, but as a baseline against which refinements, variations and alternative interpretations can be compared. A conceptual discussion of identity and e-identity, coming from a legal-philosophy perspective, is offered in IDIS by Gutwirth (2008). Ontologies and terminologies are also emerging from the computer science community: The US National Institute for Science and Technology has released a framework for the ontology of identity that attempts to circumscribe the terminology describing identity (NIST 2006) and an ongoing effort at proposing a consolidated terminology for Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management is another example of the same (Pfitzmann and Hansen 2008). Finally, a more multidisciplinary attempt undertaken as part of the FIDIS project is found in Nabeth (2005) offering of an inventory of Identity terms, but clearly, more needs to be done for proper research foundations.

### Digital identity management

Identity management has been recognized as a key research theme for the coming decades (Dunleavy et al. 2006, p. 251). For almost every organization in the future, both public and private sector, identity management presents both significant opportunities and risks (Birch 2007). Identity management broadly refers to the management of digital identities or digital identity data. Approaches to identity management differ in terms of management procedures (who is doing what and what are the possible operations on the data) and the types of data being stored and managed (e.g., comprehensive profiles of individuals or groups or a selection of

roles or partial identity—the kind of personal information known to the system). The links between different IdMS is a crucial matter for identity management—we have already highlighted interoperability as a key issue in this area—the sharing of identity data across systems, which is seen to offer certain benefits but not without significant risks, not least to safety and privacy (cf. Anderson et al. 2006).

The market for IdMS and related technological development is expanding and expected to grow fast over the coming years. Some specific types of such technologies and applications include CRM (customer relationship management, SSO (single sign-on) or indeed smartcards, RFID chips, and biometrics. Classes and typologies for IdMS have been suggested and these may be used to draw out research issues for identity management. For example, a typology of three kinds of IdMS emerged from the FIDIS research project. The three types—IdMS for accounting; IdMS profiling and User-controlled IdMS—arose from reviewing identity management systems currently available on the market as well as IdMS prototypes and concepts, and identity management-related tools (Bauer et al. 2005). Whilst type 1 and type 2 are normally utilized by large organizations or enterprises and are marked by centralized management, type three IdMS is instead user-controlled and characterizes IdMS which are decentralized, user- and client-oriented so that the personal data is typically managed by the user. Similarly, whilst type 1 and 2 focus on reliability and data integrity—type 3 IdMS brings forth mechanisms with respect for privacy—mainly the integration of privacy enhancing technology (PETs) for IdMS. However, there is evidence of this typology breaking down as new systems are developed.

## Identity systems and power structures

Changes to power structures in relation to the use of identity systems emerge as an important theme deserving research attention. Moves toward the surveillance society and consequent erosion of privacy suggest that individuals are seriously at a disadvantage in controlling the effects of surveillance whether consequences are intended or not (Wood 2006).

Lyon (2007) argues that the politics of personal information is becoming increasingly prominent (2008:450). Power relations are intrinsic to ICT enabled surveillance processes, the processing of personal data for the purposes of care or control, to influence or manage persons or populations, which brings to bear large and urgent questions about social sorting and digital discrimination (Lyon 2005; 2007).

Major risks associated with profiling activities (see in this IDIS volume the article by Hildebrandt 2008) may be understood in terms of shifts in power structures. Profiling enables those with power—businesses, governments, employers—to enhance that power, by making ever more precise decisions that benefit themselves rather than the consumer, the citizen, or employee. Individual and social groups may experience loss of control and of legal recognition, social exclusion and discrimination e.g. as a result of profiling performed in the name of national security.

At the same time, the notion of counter-profiling has been proposed as a possible way of restoring the balance of power between individual consumers and citizens on the one hand and corporations and governments on the other; shifting it yet again and perhaps empowering the citizens, consumers, employees and what is referred to

as 'traditionally weak party'. This may be achieved through the use of transparency tools given to individuals as they have never had before (Koops 2006). Yet, the ultimate effects of the use of IdMS on power relations calls for empirical research and remains to be studied.

The themes outlined above represent more focused preoccupations, or sub-topics that cut across boundaries, but still lie within the broad area of identity. Under Themes we mentioned conceptual foundations, identity management and identity systems and power structure for which many different social groups and contexts may be identified such as Immigration, Gender and Digital Refuseniks. But other important themes include, e.g. identity-related crime (Koops and Leenes 2006; Holtfreter and Holtfreter 2006; van der Meulen and Koops 2008; Marron 2008); Identity and social networks (Albrechtslund 2008) and biometric identification (Wayman 2001; van der Ploeg 2003; Zureik 2004; Prabhakar et al. 2003; Alterman 2003), to name just a few. Through the category of themes we should aim to identify those themes that appear to merit dedicated research effort. Themes can then be evaluated in terms of magnitude and importance and the extent to which they require more—or less—attention in research.

## Application areas of technology-based identity systems

A growing number of application domains appear relevant to studies of identity in the information society, highlighting the significance of sectoral analysis in this emerging field of research. Although some unifying principles may be applicable across sectors and domains and indeed are being consciously propagated, such as business models and applications being implemented in eGovernment that are borrowed from the business sector (Fountain 2001; Warner and Hefetz 2002; Ciborra 2005; King and Cotterill 2007), it is still early days to draw conclusions about the experience of identity management systems across entire sectors of public or corporate life.

The past years have witnessed a more sophisticated use of personal information to deliver a variety of services, to drive and achieve different goals. Identity has become "the new money" (Crosby 2008) as increasing exploitation of identity information through deployment in ICT penetrates more and more areas with considerable effect. Government, Healthcare, Business/commerce and the Finance sector are prominent examples briefly discussed now.

### Government

Many countries have already developed and distributed an electronic identity (eID) card (Austria, Belgium, Spain) or are announcing them (like the Netherlands[7] and the UK). In the USA, nationwide identity systems have been proposed with renewed interest in the wake of September 11, 2001 as a solution for problems ranging from counterterrorism to fraud detection to enabling electoral reforms (Kent and Millett

[7] ec.europa.eu/idabc/servlets/Doc?id=21189

2002). The ID cards will often contain some biometric of the individual concerned—a retina scan, fingerprints and so forth. Some, for example in Belgium, also contain a digital certificate and a digital signature, both implying strong identification and authentication checks certified by a Certification Authority[8]. At the same time as more European states begin to develop identity cards for identity management, the European Union has been pushing its interoperability agenda in both eHealth and eGovernment as part of its aim to support the mobility of EU citizens and develop seamless provision of government and health services no matter the location in Europe[9]. The EU's Lisbon 2000 Strategy set out the principles that should guide development of eIDs: building trust, enhancing usability, improving access and applications and services.

As eGovernment and its successor transformational government (tGovernment) (Saxby 2006) increasingly rely on personal information (Lips 2007), the introduction of public sector IDMS brings with it more predicted conflicts and tensions (see in this IDIS volume: Taylor et al. 2008) as well as new information risks (Backhouse and Halperin 2008).

### Healthcare

Replacing paper-based patient care records with electronic records has pushed healthcare into the lead for identity management application areas. eHealth is predicated on the management of electronic identities and very large sums are being invested in it. ConnectingforHealth, the biggest ICT project in the world under way in the UK National Health Service (Brennan 2007), was originally costed at £6.2 billion but this figure will double on current estimates[10]. Identity management systems in eHealth manifest themselves particularly in patient care records systems and often form the centrepiece of an eHealth strategy, enabling healthcare workers to get access to a patient's medical data regardless of their location. This approach however raises considerable problems in maintaining confidentiality whilst still providing wider access and availability. Systems on the grand scale envisaged in the UK are also raising concerns about the right technical platform, with lengthy identification and authentication processes for doctors perhaps inducing the sharing of smart cards and similar credentials with other health workers.

### Commerce/business

Identity management systems are a vital marketing tool for many commercial enterprises. A new breed of businesses is emerging whose primary business is the collection of personal digital information. For example, Wiland Services in the US has constructed a database containing over 1,000 elements, from demographic information to behavioural data on more than 215 million people (Solove 2006). Experian is another example of the same whose "principal line of business is

[8] http://www.eid-forum.be/public-faq.php

[9] http://ec.europa.eu/idabc/en/chapter/5883

[10] http://www.timesonline.co.uk/tol/news/uk/article675669.ece

providing consumer information, chiefly by using credit ratings, but it collects other information such as company records, insurance information, vehicle details and lifestyle data"[11].

Transaction data provide priceless raw material for group and individual profiling such that companies can tailor their offers and channel them to ever more narrowly defined cohorts of customers, instead of costly and bothersome scattergun dissemination (Lace 2005). Online purchasing produces a wealth of data about the customer that only need to be marshalled and mined in order to fine-tune the sales pitch (Zarsky 2002–2003). Furthermore, many systems such as mobile telephone, telecom provision, online banking, even tax return systems permit the data subject to update their personal data, such as address changes, or changes in personal circumstances. In this way an element of control over the data integrity is handed to the data subject in return for having the input provided for free. Of course, in many commercial systems the pressure for verification of personal information is much less than in eGovernment or eHealth. The commercial companies are interested in individuating their customers and maintaining a relationship with them, and not in strongly identifying and authenticating them.

### Finance

However if the company is in the financial sector, a different logic applies. Finance is therefore another application area for identity research. Anti-money laundering regulation has stiffened the sinews of the compliance departments such that every customer must undergo an extremely thorough identity check both at the start and at various times during the banking relationship. Because bank accounts are important vehicles for the hiding and laundering of illegal monies (Linn 2005), anti-money laundering regulations worldwide enjoin financial institutions to make regular sweeps of all transaction data to identify suspicious transactions and possible criminal activities. Even taking out a loan or mortgage will involve strong verification checks on identity as this is a method for laundering money. In the UK, Money Laundering Reporting Officers who fail to discharge adequately their legal obligations are at risk of imprisonment and this fact, understandably, has altered priorities greatly. The AML identity checking controls have been imposed onto ever more sectors of the economy—insurance, lawyers, accountants, estate agents—all must now report suspicious transactions and therefore must be vigilant in their management of identity systems.

We conclude that the rapid take-up of identity management systems in many application areas sends us the message of how central they are to the emerging information society. The more application areas are colonised by this technology, the more ineluctable is its destiny. From a minor player of just a few years ago, IdMS have become a real power in the land. From call centre to call centre, from help desk to technical support, from tax office to transport ticketing systems, there is no hiding place.

In the category of Application Areas we mentioned government; health care; business; finance, but there are others, including: law enforcement, crime-detection and forensics (Geradts and Sommer 2006); Human Resources/employment; education; road traffic. New application areas betoken the march of identity, the

[11] http://en.wikipedia.org/wiki/Experian

spread of IdMS, how fast they are percolating through society, how they are impacting a growing variety of professional practice and economic and social structures. The nature of such an impact and its consequences warrants research.

## Research focus

A review of the research focus driving the FIDIS research project points up the *diversity* of topics and to the broad scope of identity as a research area; from the very technical: *What are the tools (technical solutions) that can be used to support the management of identity and identification*?—to the socio-legal: *What are the societal impacts of identity-related crime*? The research focus reveals the differing units of analysis relevant to studies of identity. For example, of persons in different roles (e.g. citizen; consumer; employee; student; patient) in different places (home; work; on the move) and in different modes (offline; online; mixed modes). The significance of different *contexts* arises in proposed explorations of identity, traversing from the individual through to the organizational, the national, international and the global.

Given that identity research is still in its early days, much research is geared towards *conceptual* investigations aimed at establishing the grounds on which further research may be build. For example, the work of Nabeth (2005) questions the 'identity of identity', and attempts to firm up the conceptual foundations—a taxonomy of concepts for the identity domain. A crucial distinction is proposed between identity (understood as the set of characteristics or attributes which represent a person) and identification (the disclosure of identity information) as well as definitions for a growing set of related concepts. Within more thematic or focused studies such as profiling, the focus for example may be conceptualising ambient law (Hildebrandt and Koop 2008) or consolidating emerging notions surrounding the virtual person in order to inform further research into human and non-human legal actors (Jaquet-Chiffelle 2008). Empirical studies are emerging but so far are the minority, as perhaps might be expected, but the focus, by turns, is shifting from the technological artifact *per se* to the social, legal and cultural hinterland in which the technology thrives as *What* questions gradually give way to *How much* or *How far* questions. In the technical domain the research is driven, appropriately, by the emergence and consolidation of new artifacts.

Noticeable too is the yet small contribution from quantitative research. Without wide agreement on what the units are, counting becomes a fraught activity: i.e. more consensus is needed about the taxonomy and concepts before quantitative research will make itself felt. This might also explain the gap in empirical studies. More agreement is needed in the research community about what the relevant frameworks and theories might be. At the same time, research should not be solely concept driven but also attend to real-life vulnerabilities in identification infrastructures.

## Disciplinary approaches for identity research

This section considers the relevance of different disciplinary perspectives, and the use of related theories, conceptual frameworks and models to inform research into

identity in the information society. It also addresses the interrelated subject of *approaches* to studies in identity that result in some ambiguities regarding the nature of research in this area in terms of knowledge production and of epistemological underpinnings.

Under the social sciences umbrella, an assortment of related disciplines and fields has mustered. Among them are information systems (socio-technical approaches in particular); management; economics; organisation theory; psychology; sociology; government and political science; social policy and others. For example, psychology and sociology have tackled the concept of identity as the construction of the self for the individual (e.g., Giddens 1991; du Gay 2007), and the development of shared values and norms associated with the identity of groups or social collectives; organization studies associate identity with forms of identification and the definition of roles.

Lawyers and legal philosophers have addressed the issue of identity in connection with responsibility, privacy and data protection, constitutional democracy, ethics and morality. Law and policy scholars are exploring ways in which law regulates anonymity and privacy—when law permits anonymity, when it imposes anonymity, when it requires identification (Kerr and Young 2005).

Finally, the technological perspective addresses questions of authentication, identity representation, and identity protection in applications of, for example, Privacy Enhancing Technologies (PETs). It explores new and emerging technologies that could revolutionise the interface of conflict between information harvesting and the maintenance of security and privacy. An interesting development is the move for ICT to incorporate and inscribe the regulatory norms within its own configuration, requiring the transcription of legal norms into programmed format, perhaps including algorithmic operations. Even without this, identity management has become such a mammoth and yet crucial task for modern organizations that technology innovation in this area is bound to be vibrant for some years. The functions of identification and authentication on which so much selection and protection is based will have to be increasingly automated, if the throughput of individuals is to be handled in a cost-effective and efficient way.

But clearly, these perspectives are not mutually exclusive; each of them can shed interesting and complementary light on the same problematic and should not, therefore, be treated separately. For instance, the problem of managing access to restricted resources can and should be addressed in many different ways: computer scientists can propose authentication mechanisms, such as biometrics; sociologists can offer input on behaviour (and help to identify suspect behaviours); organization experts can contribute to the definition of roles in the organization or system and to the definition of level of access to resources that enhance the protection of confidential information. By articulating the rights of users and the sanctions associated with unauthorized behaviour, lawyers can contribute to resolving issues of access to restricted resources.

Following this example, the notion of *Mode 2 research* introduced by Gibbons et al. (1994) might be useful for characterising desirable knowledge production processes in the identity domain. Mode 2 refers to a form of knowledge production that is context-driven, problem-focused and interdisciplinary. It involves multidisciplinary teams brought together to work on specific problems in the real world.

Mode 2 is distinguished from traditional research, labelled 'mode 1', which is academic, investigator-initiated and discipline-based knowledge production. If we contend that research in identity should be context-driven and problem-based in the Mode 2 sense then collaborative, interdisciplinary research seems desirable, indeed necessary, for achieving a multifaceted and rounded understanding of the identity domain. However this is not the prevailing trend. Research in identity is currently fragmented along disciplinary lines. A comprehensive review of the literature highlights the discipline-bound nature of the research on identity and the prevailing boundaries (Halperin 2006).

Barriers to interdisciplinary research are numerous and beyond the scope of this paper as a general problem. Still, it has been argued that a common vocabulary for the identity domain might help overcome some of the barriers (Nabeth 2005). But can a unified vocabulary tackle the underlying problem of multiple interpretations and differing epistemologies associated with different disciplinary perspectives? Although similar terms may be used by different researchers, wide divergence emerges when concepts are interpreted and applied in research studies. For example, information security in engineering terms is ultimately viewed as a mechanism. For IS researchers adopting a socio-technical perspective, security is instead understood as a social process with technical mechanisms to support it. It is seen as the response to risk, with countermeasures, practices and norms (Dhillon and Backhouse 2000).

Significant gaps become apparent when examining existing pieces of research in the identity field in terms of conceptual models and the theories that underpin them. Hence *Trust*, a vital issue for this topic, requires theorising and operationalizing to be studied in the context of Identity. Definitions range for example across ethics-based approaches at the qualitative end of the spectrum to economics-based approaches at the numerical end (Zucker 1986; Metlay 1999; McKnight et al. 2002; Pavlou 2002). Such conceptions rest typically on distinct ontological and epistemological foundations that may not be easily reconciled.

When delineating the problem domain, levels of tolerance to ambiguity, uncertainty and emergence phenomena are another dimension in which disciplinary gaps become evident. Whilst technologists often require finite, objectified models to allow the design and construction of computer-based systems, socio-cultural analysis draws attention to drift (Ciborra 2000), volatility and the dynamics associated with the conception, implementation and appropriation of information systems (Orlikowski 2000), and the contextual particularities of their use (Avgerou 2001; Avgerou and Madon 2004).

Note, however, that the tendency to study identity from a single, disciplinary point of view may generate obvious advantages in terms of depth and rigour. Quality research, it may be argued, can only come from within disciplinary confines. If intellectual coherence, consistency and rigour are the hallmarks, then interdisciplinary research remains a formidable challenge. We maintain that the nature of identity (as a concept and a phenomenon) is such that a multifaceted approach to its study should be fostered, by means of collaborative research (cf. Koops et al. 2008) and certainly, by sharing results and findings among the heterogenous community of researchers that exists. This is perhaps the fundamental requirement for a rounded understanding to emerge. Cross-disciplinary exchange has been proposed as another way forward. A recent book from the FIDIS project entitled 'Profiling the European

Citizen' (Hildebrandt and Gurtwith 2008) is an illustration, where each chapter is followed by a critical reply fashioned by a scholar from a different discipline. While the cross-disciplinary model does not cater for the integration of different disciplinary perspective into a single piece of research or a research project, it does allow for both pluralism and criticism in the discourse.

What can we learn from exploring the role of disciplines and approaches in studies of identity? First, by considering the relevance of disciplinary perspectives we are able to identify the *community of interest* and to specify the kind of *expertise* required for comprehensive research in the identity area. It is becoming clear that inclusive coverage and a full understanding of the identity domain requires a growing array of expertise that cuts across specialist fields and disciplinary lines. The need for diversity in knowledge and expertise for researching in this field is further underlined by the previous discussion on the wide-ranging areas of application associated with the identity field. Context-specific knowledge in these domains, be it health care, government or crime detection, is needed to support rigorous research in this field.

Second, viewing the identity field as requiring a mode 2 knowledge production process encourages us to consider ways of fostering collaborative research in this field whilst drawing attention to some of the challenges involved, in particular, developing a shared terminology and understanding across disciplines, overcoming epistemological divides and ensuring rigour, validity and reliability of research studies. Notwithstanding this, researchers must urgently redouble their efforts in order to answer the more difficult questions about how different perspectives might be reconciled before a balanced and holistic approach to the pressing contemporary issues of identity may emerge.

## Concluding remark

The IDIS journal marks an exciting phase in the development of studies into identity in the information society. Its launch betokens the existence of a substantial community of scholars and practitioners who are interested in reading articles and in contributing to the debate on identity issues. This paper has essayed an overarching view of identity research, setting out five distinctive perspectives that enable the various elements and streams of intellectual and professional activity to be reconciled in an integrated fashion. It does not attempt to be comprehensive as this would be impossible in the space of a journal article, but it offers a roadmap of where research is currently placed and where it is moving towards. The challenge is for this initial sketch to be criticized, strengthened and improved.

## References

Albrechtslund A online social networking as participatory surveillance, first Monday (13:3) 2008, http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2142/1949.

Alterman A. "A piece of yourself": ethical issues in biometric identification. Ethics Inf Technol. 2003;5:39–150.

Anderson R. Under threat: patient confidentiality and NHS computing, www.cl.cam.ac.uk/~rja14/Papers/drugsandalcohol.pdf) 2007.
Anderson R, Brown I, Clayton R, Dowty T, Kroff D, Munro E. Children's databases—safety and privacy. Information Commissioner's Office; 2006.
Anilik J, Ross A. Multibiometric systems. Commun ACM. 2004;47(1):34–40.
Avgerou C. The significance of context in information systems and organizational change. Inf Syst J. 2001;11:43–63.
Avgerou C, Madon S. Framing IS studies: understanding the social context of IS innovation. In: Avgerou C, Cibbora C, Land FF, editors. The social study of ICT. Oxford: Oxford University Press; 2004. p. 162–82.
Backhouse J. Interoperability of identity and identity management systems. Data Protection and Data Security. 2006;30(9):568–70.
Backhouse J, Halperin R (eds) EU Citizen's trust in future ID systems and authorities. FIDIS Deliverable 4.4/4.5. Available at: fidi.net, 2007.
Backhouse J, Halperin R. Security and privacy perceptions of eID: a grounded research. European Conference on Information Systems. Galway, Ireland; 2008a.
Backhouse J, Halperin R. Approaching interoperability for identity management systems. In: Rannenberg K editor. Identity in the information Society: challenges and opportunities. Springer, Berlin; 2008b (in press).
Bauer M, Meintz M, Hansen M (eds) Prototypes and concepts of identity management systems. FIDIS Deliverable 3.1. Available at: Available at: fidis.net, 2005.
Birch D (ed) Digital identity management. Gower, Hampshire; 2007.
Brennan S. The biggest computer programme in the world ever! How's it going? J Inf Technol. 2007;22:202–11.
Brubaker R, Cooper F. Beyond identity. Theory and Soc. 2000;29:1–47.
Cavoukian A. Privacy and radical pragmatism: change the paradigm, a white paper information and privacy commissioner of Ontario, Canada; 2008.
Ciborra C. From control to drift. Oxford: Oxford University Press; 2000.
Ciborra C. Interpreting e-government and development: efficiency, transparency or governance at a distance? Inform Tech People. 2005;18(3):260–79.
Clarke R. Disidentity. Identity in the Information Society 2008;1(1) (in press).
Crosby SJ. Challenges and opportunities in identity assurance. http://www.hm-treasury.gov.uk/media/6/7/identity_assurance060308.pdf, 2008.
Crossman G. The ID problem. In: Birch D, editor. Digital identity management. Hampshire: Gower; 2007. p. 175–83.
Dhillon G, Backhouse J. Information system security management in the new millennium. Comm ACM. 2000;43(7):125–8.
Dowty T. Overlooking children: an experiment with consequences. Identity in the Information Society 2008;1(1) (in press).
Du Gay P. Organizing identity. London: Sage; 2007.
Dunleavy P, Margetts H, Bastow S, Tinkler J. Digital era governance. Oxford: Oxford University Press; 2006.
Eckfeldt B. What does RFID do for the consumer. Comm ACM. 2005;48(9):77–9.
Etzioni A. Applications of select new technologies for individual rights and public safety. Harv J Law Technol. 2002;15(2):34.
Fountain JE. Paradoxes of public sector service, governance. International Journal of Policy and Administration. 2001;14(1):55–73.
Galliers RD. Change as crisis or growth? Toward a trans-disciplinary view of information systems as a field of study: a response to Benbasat and Zmud's call for returning to the IT artifact. J Assoc Inform Syst Online. 2003;4(6):337–51.
Geradts Z, Sommer P (eds) Forensic implications of identity management systems. FIDIS WP6 Deliverable 6.1. Available at: fidis.net, 2006.
Gibbons M, Limoges C, Nowotny H, Schwartzman S, Scott P, Trow M. The new production of knowledge: the dynamics of science and research in contemporary societies. London: Sage; 1994.
Giddens A. Modernity and self identity. Cambridge: Polity; 1991.
Gutwirth S. Beyond identity. Identity in the Information Society 2008;1(1) (in press).
Halperin R. Identity as an emerging field of study. Data Protection and Data Security. 2006;30(9):533–7.
Hildebrandt M. Profiling and the rule of law. Identity in the Information Society 2008;1(1) (in press).
Hildebrandt M, Gurtwith S (eds) Profiling the European Citizen. Springer, Berlin; 2008.
Hildebrandt M, Koops BJ (eds) A vision for ambient law. FIDIS Deliverable D7.9 Available at: fidis.net, 2008.

Holtfreter RE, Holtfreter K. Gauging the effectiveness of US identity theft legislation. J Financ Crime. 2006;13(1):56–64.
Jaquet-Chiffelle DO (ed) Virtual persons and Identity? FIDIS Deliverable D2.13. Available at: fidis.net, 2008.
Kent S, Millett LI (eds) IDs—not that easy: questions about nationwide identity systems. committee on authentication technologies and their privacy implications. National Research Council 2002.
Kerr I, Young H. Two years on the identity trail. Canadian Privacy Law Review 2005.
Kinder T. Mrs Miller moves house: the interoperability of local public services in Europe. J Eur Soc Policy. 2003;13(2):141–57.
King S, Cotterill S. Transformational government? The role of information technology in delivering citizen-centric local public services. Local Govern Stud. 2007;33(3):333–54.
Koops B. Counter-profiling by 'weak' parties. In: Hildebrandt M, Gutwirth S, De Hert P, editors. Implications of profiling practices on democracy and rule of law. FIDIS Deliverable D7.4 Available at: fidis.net, 2006.
Koops B, Leenes R. Identity theft, identity fraud and/or identity-related crime. Data Protection and Data Security. 2006;30(9):553–9.
Koops B, Leenes R, Meints M, van der Meulen N, Jaquet-Chiffelle, DO. A typology of identity-related crime: conceptual, technical, and legal issues. Inform Comm Soc 2008 (in press).
Kramer RM. Trust and distrust in organizations: emerging perspective, enduring questions. Annu Rev Psychol. 1999;50:569–98.
Lace S (ed) The glass consumer: life in a surveillance society. UK: Policy Press; 2005.
Lessig L. Code and other laws of cyberspace basic books. New York: Basic Books; 1999.
Linn CJ. How terrorists exploit gaps in US anti-money laundering laws to secrete plunder. J Money Laund Control. 2005;8(3):200–14.
Lips AMB. E-government under construction: challenging traditional conceptions of citizenship. In: Nixon P, Koutrakou V, editors. E-government in Europe rebooting the state. London: Routledge; 2007. p. 33–47.
Lyon D (ed) Surveillance as social sorting: privacy, risk and digital discrimination. London: Routledge, 2005.
Lyon D. Surveillance, power, and everyday life. In: Mansell R, Avgerou C, Quah D, Silverstone R, editors. The Oxford handbook of information and communication technologies. Oxford: Oxford University Press; 2007. p. 449–72.
Marron D. Alter reality: governing the risk of identity theft. British Journal of Criminology. 2008;48:20–38.
McKnight DH, Choudhury V, Kacmar C. Developing and validating trust measures for E-commerce an integrative typology. Inf Syst Res. 2002;13(3):334–59.
Metlay D. Institutional trust and confidence: a journey into a conceptual quagmire. In: Cvetkovich GT, Löfstedt RE, editors. Social trust and the management of risk. London: Earthscan; 1999. p. 100–16.
Nabeth T (ed) Inventory of topics and clusters. FIDIS Deliverable 2.1. Available at: fidis.net, 2005.
NIST. Information security—an ontology of identity credentials, part 1: background and formulation. Washington, USA: National Institute for Technology Administration, U.S. Department of Commerce; 2006.
Orlikowski WJ. Using technology and constituting structure: a practice lens for studying technology in organizations. Organizational Science. 2000;11(4):404–28.
Otjacques BPH, Feltz F. Interoperability of e-government information systems: issues of identification and data sharing. J Manage Inf Syst. 2007;(23:4):29–51.
Pavlou PA. Institution-based trust in interorganizational exchange relationships: the role of online b2b marketplaces on trust formation. J Strateg Inf Syst. 2002;11(3):215–43.
Pfitzmann A, Hansen M. Anonymity, unlinkability, unobservability, pseudonymity, and identity management—a consolidated proposal for terminology. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf.
Pounder C. Nine principles for assessing whether privacy is protected in a surveillance society. Identity in the Information Society 2008;1(1) (in press).
Prabhakar S, Pankanti S, Jain AK. Biometric recognition: security and privacy concerns. IEEE Secur Privacy. 2003;1(2):33–42.
Royal Academy of Engineering. Dilemmas of privacy and surveillance: challenges of technological change. London: RAE; 2007.
Saxby S. eGovernment is dead: long live transformation. Comput Law Secur Rep. 2006;22:1–2.
Schneier B. Beyond fear. New York: Springer; 2006.

Scholl HJ. Interoperability in E-government: more than just smart middleware. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005. IEEE, Hawaii, 2005;123–123.

Six P, Raab C, Bellamy C. Joined-up government and privacy in the UK part I: managing tensions between data protection and social policy. Part I. Public Administration. 2005;83(1):111–33.

Solove D. The digital person and the future of privacy. In: Strandburg K, Stan Raicu D, editors. Privacy and technologies of identity—a cross-disciplinary conversation. New York: Springer; 2006.

Taylor JA, Lips M, Organ J. Identity in the Information Society 2008;1(1) (in pres)

van der Meulen N, Koops BJ (eds) Identity-related crime in Europe—big problem or big hype?" FIDIS Deliverable D12.7. Available at: fidis.net, 2008

van der Ploeg I. Biometrics and privacy: a note on the politics of theorizing technology. Inf Commun Soc. 2003;6(1):85–104.

Warner M, Hefetz A. Applying market solutions to public services: an assessment of efficiency, equity and voice. Urban Aff Rev. 2002;38(1):70–89.

Wayman JL. Fundamentals of biomentric authentication technologies. Int J Image Graph. 2001;1(1):98–113.

Wood DM (ed) A report on the surveillance society. Information Commissioner Office, 2006.

Zarsky T. Mine your own business! Yale Journal of Law and Technology 2002–2003;5:17–47.

Zucker LG. Production of trust: institutional sources of economic structure: 1840–1920. Res Organ Behav. 1986;8(1):53–111.

Zureik E. Governance, security and technology: the case of biometrics. Stud Polit Econ. 2004;73:113–37. (with contribution from Karen Hindle, Spring/Summer).