IDIS (2010) 3:605–638
DOI 10.1007/s12394-010-0078-3

A framework for the lived experience of identity

Adrian Rahaman · Martina Angela Sasse

Received: 29 June 2010 / Accepted: 25 October 2010 / Published online: 20 November 2010

Abstract This paper presents a framework for the design of human-centric identity management systems. Whilst many identity systems over the past few years have been labelled as *human-centred,* we argue that the term has been appropriated by technologists to claim moral superiority of their products, and by system owners who confuse administrative convenience with benefits for users. The framework for human-centred identity presented here identifies a set of design properties that can impact the lived experience of the individuals whose identity is being managed. These properties were identified through an analysis of public response to 15 historic national identity systems. They capture the practical design aspects of an identity system, from structural aspects that affect the flow of information - *Control Points, Subject Engagement, Identity Exposure, Population Coverage*—to the metrical aspects that considers how information is used and perceived—*Expert Interpretation, Population Comprehension, Information Accuracy, Information Stability, Subject Coupling, Information Polymorphism*. Any identity system can be described in terms of these fundamental properties, which affect individuals' lived experience, and therefore help to determine the acceptance or rejection of such systems. We first apply each individual property within the context of two national identity systems—the UK DNA Database and the Austrian Citizen Card, and then also demonstrate the applicability of the framework within the contexts of two non-government identity platforms—Facebook and Phorm. Practitioners and researchers would make use of this framework by analysing an identity system in terms of the various properties, and the interactions between these properties within the context of use, thus allowing for the development of the potential impacts that the system has on the lived experience.

Keywords Identity · Identity management system · Privacy · Trust · Design · Lived experience

A. Rahaman (✉) · M. A. Sasse
Computer Science, University College London, London, UK
e-mail: a.sallehabrahaman@cs.ucl.ac.uk

M. A. Sasse
e-mail: a.sasse@cs.ucl.ac.uk

Introduction: identity systems today

Identity is a construct that underlies the mechanisms which enable or prevent an individual from performing certain actions in a social environment. Many organisations seek to obtain—explicitly or implicitly—reliable proof of individuals' identities, to ensure effective policing of their rules and policies. Ashbourn (2000) describes how administrators in ancient Egypt used anthropometric techniques to identify workers claiming their food rations, to prevent them collecting rations more than once. Anthropometric techniques were used in France as a means of identifying recidivists, so authorities could give them harsher sentences than first-time offenders (Caplan and Torpey 2001). With the increasing use of IT systems, there is a growing disembodiment of identity processes; interactions that were previously conducted face-to-face, and using physical documents as evidence, are now mediated through information and communication technology (Giddens 1991; Lyon 2002). There has been a flurry of research in how to best represent and manage identities in this context, and a number of different schemes and technologies have been proposed, designed and implemented.

In the private sector, the eagerness to identify individuals and collect information about them is driven by the promise of new revenue streams through the provision of 'customer-centric' personalized services. Recommender and social networking systems rely on the aggregation of various types of information about individuals—the resulting identity profiles allow third parties to judge the trustworthiness and the authenticity of each respective individual (O'Donovan and Smyth 2005). The public sector wants to harness similar approaches to reduce the costs of service delivery and increase convenience through 'citizen-centric' services and data-sharing (Silcock 2001).

There is however, a risk that the labels 'customer-centric' or 'citizen-centric' remain a statement of intent, because the *needs and wishes* of individual customers and citizens, and the impact of identity systems on their *lived experience,* are rarely considered during the design process. The concept of *lived experience* increases the scope of human-centred design beyond traditional usability concepts, which are *"directed more toward functional accounts of computers and human activities"* (McCarthy and Wright 2004). Designing for the lived experience requires an understanding of "*the relationship between people and technology in terms of felt life and the felt or emotional quality of action and interaction*" (McCarthy and Wright 2004). Current approaches to human-centered identity do not consider the impact on lived experience. For example, in a report sponsored by the Information Commissioner's Office (Workgroup on User-Centric Identity Management 2008), discussions on empowering individuals were focused on the 3 traditional pillars for human-centred design:

1) Usability—Making identity systems simple and easy to use reduces barriers to adoption.
2) Privacy—Privacy concerns are a major factor in the adoption of identity systems. These systems can involve the transfer of sensitive information between different parties. Protecting privacy is important so as to prevent personal information from falling into the wrong hands which can erode autonomy and freedom.

3) Trust—The degree of trust that individuals have in the organisation collecting identity information mediates their concerns about privacy. High trust will increase adoption of an identity system (Adams and Sasse 2001).

The discussions of the three aspects of identity systems are utilitarian—essentially seeking to enable organisations to obtain individuals' consent for collection and sharing of information. It does not consider the more far-reaching impact of the use of identity information on individuals, reducing the 'human-centred' discussion to the technological issues surrounding data collection, and administrative benefits for organisations. Not considering citizens' needs and perceptions can affect the adoption of such systems. Inglesant and Sasse (2007) conducted a series of case studies on e-government systems commissioned to improve public transport in London, and found that design and implementation decisions led to systems that did not match citizen requirements, and often prompted citizen behaviour that undermined the policy those systems were supposed to support. This affects adoption rates systems, and even in situations where citizens have little choice but adopt them—creates an adversarial stance between the citizens and the owner-organisation, which in turn increases the operational cost of such systems. Given that many e-Government systems are commissioned to reduce cost, systems that create an adversarial stance are counter-productive.

While citizens and customers have accepted some of the new identity systems, they have also voiced their disagreement in other cases. Facebook users protested when profile updates were broadcast (Hoadley et al. 2009), and there have been campaigns against the introduction of national identity systems (Greenleaf and Nolan 1986; The Register 2002; Davies 2005). In other cases, such as the Austrian Citizen Card (Meints and Hansen 2006), there has been a lack of adoption. The problem is that—despite claims that these technologies provide human-centred identity solutions—most systems have been based on what is technically feasible, and convenient from an administrative point of view. The needs and concerns of citizens or customers are often assumed by those commissioning and designing the identity solution, rather than researched (Lips et al. 2005). The impact on the *lived experience* of different citizen groups is rarely considered during design, or monitored after implementation.

In this paper, we present a framework that can be used to assess the design of an identity system from the perspective of *individuals*, accounting for the potential affects of the system on the lived experience. An *individual* here is defined as the person whose identity and information is collected, stored and used within the system. Current approaches to the development and analysis of identity systems lack understanding of how identity systems *practically* affect individuals in their day-to-day interactions within a society, and how this can affect them. The proposed framework expands beyond these traditional boundaries by shifting focus onto the *identity ecosystem* as a whole, recognizing the relationships that exist between the individual, the system and society.

In "Human-centred identity: related models", we present a critical review of existing identity management frameworks and systems that claim to be human-centred. "A new framework: discovering the lived experience of identity" describes how the framework emerged as a result of a thematic analysis of 15 past and present national identity systems. The core elements of the framework are presented in "Structural properties" and "Metrical properties". "Combining properties" discusses how those properties relate to each other, and how certain combinations within an identity system can impact individuals' lived experience.

"Applying framework to non-government identity systems" applies the properties to non-government systems—Facebook and Phorm. This serves to illustrate the generalizability of these properties and also acts as a form of validation. "Discussion and conclusion" serves as a conclusion and discussion point for the proposed framework. The strengths and weaknesses of the framework are examined, and scope for further work and improvements is provided.

Human-centred identity: related models

There is a growing body of research on identity management that focuses on the human element in identity systems. Much of the research is focussed on making identity systems easier to use (Cameron 2005; Bramhall et al. 2007; Jøsang et al. 2007), issues of privacy (Bramhall et al. 2007; Cavoukian 2009; Camenisch et al. 2005; Berthold and Köhntopp 2001) and trust (Xin 2004; Backhouse and Halperin 2007) but does not consider the impact on an individual's lived experience.

The 7 laws of identity

Developing the concept of the identity metasystem, Kim Cameron (Cameron 2005) put forward 7 rules of identity. An identity metasystem is a unifying framework that enables the integration of different underlying identification technologies, enabling different identity platforms to work through a standardized interface. These rules have become an accepted standard for identity systems. The rules that have been defined are:

1. User Control and Consent
2. Minimal Disclosure for a Constrained Use
3. Justifiable Parties
4. Directed Identity
5. Pluralism of Operators and Technologies
6. Human Integration
7. Consistent Experience Across Contexts

These 7 rules represent a foundation for eliminating the *"patchwork of identity one-offs that is currently available on the internet"* (Cameron 2005). However, they focus on individuals as *users of the system*, and tackle usability issues that individuals encounter when using identity systems; the aim is to give users control and allow them to make decisions that reflect their preferences. For example, individuals should understand which organisations will receive their information, and agree to the uses that the organisation makes of their personal information.

While Cameron's 2nd and 3rd laws on constrained use and justifiable parties address certain non-interaction issues on the use of information by the consuming party, the aim is to ensure that the individual is aware of how the information is used, and by whom. It does not consider why an individual might be reluctant to provide certain information to certain parties. While the laws provide a useful set of user-centred design principles, they do not examine the impact of the system beyond the point of interaction.

Privacy

Privacy is a multi-dimensional concept that incorporates the physical, psychological, interactional and information domain (Burgoon 1982; Davies 1997; Decew 1997). Privacy assessments of identity systems typically fall into the informational privacy domain (Smith et al. 1996). This results in a set of best use practices, which are integrated into the development of new Privacy Enhancing Technologies (PETs) (Goldberg 2003), or as guidelines for the development of laws that aim to minimise threats to privacy. Various privacy laws and standards exist: the UK Data Protection Act (DPA), the FTC Fair Information Practices (FIP), or the more recent Global Privacy Standard (GPS). The GPS has been proposed as a "*single harmonized set of universal privacy principles*". The GPS consists of 10 privacy principles (Cavoukian 2010):

1. Consent
2. Accountability
3. Specific Purposes
4. Collection Limitation (Data Minimization)
5. Use, Retention and Disclosure Limitation
6. Accuracy
7. Security
8. Openness
9. Access
10. Compliance

These principles provide a foundation for an individual's rights over the collection and use of his/her personal information by organisations. However, these codes of conduct also seek to promote business through the "*free and uninterrupted (but responsible) flow and uses of personal data*" (Cavoukian 2009). While there is a need to balance individual and organisational needs, these principles are focused on the practices of the organisation, and not on the impact to the individual. For example, the collection of information for a specific purpose does not account for the individual's perception of that purpose. In systems where participation is voluntary, the principle of consent allows individuals to act on their perceptions. However, the privacy principles do not help us to understand why individuals would not consent. While privacy principles can restrict organisational usage of an individual's data, they do not help to generate consent from the individual to provide his/her information. Individuals are considered as customers instead of actors in the identity ecosystem.

Xin's trust model

Xin (2004) developed a comprehensive model of trust that aims to predict individual trust intentions towards National Identity Systems, determining the likely adoption of the system (Fig. 1). This approach can be seen as being more human centric when compared to the 7 laws of identity and the privacy approaches seen previously. While the trust model lacks grounding in large empirical studies, its development is based on existing recognized models, such as the Theory of Reasoned Action (Fishbein 1975) and Theory of Planned Behaviour (Ajzen 1985).

An individual's trusting intention towards identity system depends on 3 assessments that the individual makes about the context:

1) the individual's positive/negative *Attitude* towards the trusting action
2) his/her judgment on the *Subjective Norms*
3) the individual's *Perceived Behavioural Control*

Each judgement, in turn, is determined by a set of behavioural, normative and control beliefs. Beliefs are the "*subjective probability of a relation between the object of belief and some other object, value, concept or attribute*" (Fishbein and Ajzen 1975). The beliefs influence the judgements:

1) *Behavioural Beliefs* influence *Attitude*
2) *Normative Beliefs* influence *Subjective Norm*
3) *Control Beliefs* influence *Perceived Behavioural Control*

Finally, beliefs are built on specific contextual properties. Building on other trust literature, Xin's (2004) developed a set of context-specific variables for National Identity Systems. These variables called 'bases' consist of the personality, cognitive, calculative and institutional base. Through empirical research, it was established that:

1) *Cognitive Base* determined behavioural and *Normative Beliefs*
2) *Calculative Base* affected the *Normative Beliefs*
3) *Personality Base* influenced the *Institutional Base*

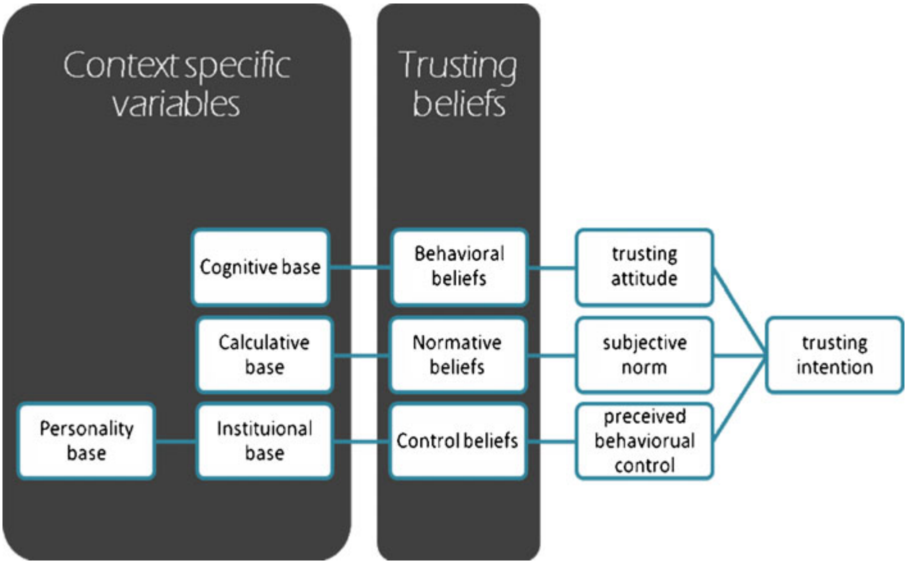

Fig. 1 Xin's trust model towards national IDMS

4) *Institutional Base* influenced an individual's *Perceived Behavioural Control.*

While the model is comprehensive, it does not support designers aiming to build a human-centred identity system since the trusting bases, attitudes and beliefs are only an individual's opinions about performing the trusting action, e.g. signing up for the National Identity System. It does not link the trust model to the actual design of the system. The contextual variables are not connected to any specific implementation details. The framework can help implementers understand an individuals' general thought processes in the development of trusting intentions, thus enabling the creation of more trusting situations. For example, recommendations to increase trust based on this model include the use of focus groups to generate positive feedback that can be publicised to manipulate the perceived reputation of the system (Xin 2004). Effectively, these recommendations are limited to the manipulation of the situational constructs that the system is implemented in, as opposed to detailing how the system itself can influence the *lived experience,* and hence trust.

Table 1 Definitions of construct's in Xin's trust model

Construct	Definition
Attitude	People's evaluation of trusting in NID systems when the government implements them nationwide in the near future.
Subjective Norm	How the people important to you think you should or should not make yourself vulnerable to NID systems when the government implements them nationwide in the near future.
Perceived Behavioural Control	Peoples perceived internal/external opportunities and constraints on being vulnerable to NID systems when the U.S. government implements them nationwide in the near future.
Behavioural Beliefs	Peoples perceptions and information about the consequences of trusting NID systems.
Normative Beliefs	Peoples perceptions and information about the others' opinions on NID systems.
Control Beliefs	Peoples perceptions of their ability, their knowledge about the recourses, opportunities, and constraints of trusting in NID systems.
Personality Base ○ Faith in humanity ○ Trusting stance	Peoples general tendency to trust an object
Cognitive Base ○ Reputation ○ Stereotyping ○ Illusion of Control	Various cognitive cues and impressions on which people form their trusts
Calculative Base ○ Benefits vs. Costs	Refers to some calculative processes involving perceived cost and benefit of performing the trusting behaviour.
Institutional Base ○ Situational Normality ○ Structural Assurance	The impersonal structures that are inherent in a specific circumstance and facilitate trust building in this circumstance

A new framework: discovering the lived experience of identity

Analyzing identity schemes from the traditional usability, privacy and trust perspective abstracts the identity system from the specific consequences that it has on individuals' lives and the various coping strategies that might be adopted. We talk about 'data minimisation' or 'ease of use', but what does it mean to an individual? How does it affect an individual's relationship with the organisation and society? The current frameworks have been useful for the development of better systems, but in applying these principles we lose sight of the entire context of implementation, i.e. the *identity ecosystem* that recognizes the relationships that exist between the individual, system and society. Therefore, the claim that an identity system is human-centred is largely rhetorical; we assume that individuals want better controls and collection of less data, but we have no idea as to how and under what conditions it affects their perceptions. For example, the advertising platform Phorm was deployed by Internet Service Providers with the intention to serve personalised advertisements, based on an individual's online browsing habits. Although privacy experts had given the system their approval, Phorm still raised privacy concerns for customers leading to protests and vigorous opposition (BBC, 2008b).

Practitioners and researchers require a way of analysing the lived experience that results from participating in an identity ecosystem. We require a framework that will allow them to assess how the designs of an identity system might influence an individual's perception of the context, and therefore how the system can shape an individual's reactions when encountering such systems.

Methodology

A tool aiming to assess the impact of an identity system design should be expressed as a set of configuration properties into which any such system can be decomposed. We have identified these properties through a review of past and present National Identity Systems. The scope of that review was limited to National Identity Systems in the Western world, largely focusing on a timeframe extending from the medieval periods to the present day, as these countries have been leading the development and adoption of modern identity systems (Torpey 2000).

The systems that formed the focus of the review (see Table 2) were implementations of Identity Systems that supported the development of Nation States, its control over migration and crime, and the provision of welfare and services. The aim of the analysis was to tie the known outcomes of each system to specific design aspects. Each system was treated as a unique case study, and a *corpus* of written work (largely from secondary sources that review the entire situation) centred on each identity scheme was collected for analysis.

Thematic Coding (Marks and Yardley 2004; Flick 2002) was used to identify similarities across the narratives of the various past and present national-scale identity schemes. Thematic coding is a qualitative research method the makes use of a constant comparison paradigm between several case studies, attempting to identify patterns that relate to the phenomena of interest. The method enables the identification of themes across different contexts from large volumes of data. Our analysis treated each national identity system as a separate case, and identified

Table 2 National identity systems analyzed

System	Country	Purpose
Poor Laws and Badges	United Kingdom	To provide members of organisations proof of association
Criminal 'Wanted' Lists	–	To provide for accurate identification of individuals especially criminals
Internal Passports	Russia	To track movement of locals in the country
Passports	Netherlands	To prevent or monitor the entry of dangerous foreign radicals into the country
French Nomad Law	France	Identification and monitoring of unwanted members of the population
National ID Cards	United Kingdom Germany	To provide unique identities to individuals allowing easy identification of the entire population.
Bertillonage	France	To identify recidivists enabling enforcement of severe punishment
Dactyloscopy	Argentina	To identify recidivists enabling enforcement of severe punishment
US Visit Programme	United States	To identify criminals and terrorists entering or leaving the country
UAE Iris Scan	United Arab Emirates	To accurately identify known individuals against captured Iris scans (e.g. criminals)
Criminal DNA Database	United Kingdom	To accurately identify individuals against DNA samples
Contact Point	United Kingdom	To identify children in need of protection services before serious harm is caused
PKI and Digital Signatures	Austria	To provide individuals access to services in a virtual environment

features of each system that led to the documented responses from the various stakeholders. The analysis took place in three main phases:

1. Reviewing an authoritative and recognized documentation of each implementation, determining the degree of adoption, and the various reactions towards the system implementation. Did individuals sign up to a voluntary system? Did they attempt to evade non-voluntary systems? Did they change their habits as a result of being part of the system?
2. Discover the arguments that lead individuals to react in the manner identified-how did they feel about the system?
3. Code the basic features, i.e. the design properties of the system that brought about the identified reactions of individuals.

As a brief example, the analysis of the use of badges under the Poor Laws in 17th century England began by identifying the theme of rejection among the individuals who were to enroll into the system (Caplan and Torpey 2001; Carroll 1996). Analysing the main documentation, and where required accompanied by relevant support material, we found that rejection stemmed from feelings of shame that arose from being registered in the scheme. We can then identify the characteristics of the system that triggered these emotions the feelings of shame were triggered by the constant wearing of the badges, which exposed a small set of individuals to the rest of the population.

These system characteristics formed the basis of the coding procedure in the analysis. The codes were developed to express basic design aspects of an identity system. Using the above example, we code 'the need to constantly wear badges' as a design property that is expressed as *Control Points*; *Control Points* capture the number of places where identity is required to proceed with some action. The exposure of the identity to the rest of society is captured by the code *Identity Exposure*; this property expresses how much control an individual has in the presentation of the identity to the rest of society. Finally, the small set of individuals enrolled in the system is captured by the concept of *Population Participation*; the ratio of individuals enrolled into the system to the rest of the population that are not enrolled.

The codes have been developed to express a measure of the amount of relevant affordances that the system can provide for each property. Therefore, the Poor Laws with the badges would have a high number of *Control Points*, a high degree of *Identity Exposure* and a low level of *Population Coverage*. It is the interaction of these design properties that brings about the feelings of shame that were identified as the cause of rejection.

Further analysis of all the codes, revealed that the design properties can be distinguished into two main categories: structural properties and the metrical properties (see Table 3). Structural properties focus on the design aspects that capture the flow and relationship of an individual's information within the identity ecosystem created. Metrical properties are based on the qualities that are affected by the type and amount of information that is being collected and used in the identity system.

Setting the context

In this section, we introduce two identity systems that were used in the thematic coding process—UK DNA Database and the Austrian Citizen Card. An outline of the basic implementation details and the eventual outcomes is provided for both identity systems. This section does not touch on any of the properties that have been uncovered, but serves as a base for contextualising the properties when they are introduced in the following sections. Doing so is useful, as it allows the later introduction of each property to be discussed and elaborated upon within a particular context.

Table 3 System properties

Structural properties	Metrical properties
Control Points	*Population Comprehension*
Subject Engagement	*Expert Interpretation*
Identity Exposure	*Information Accuracy*
Population Coverage	*Information Stability*
	Subject Coupling
	Information Polymorphism

The UK criminal DNA database is an identity system consisting of a central database that stores an individual's DNA sample, and creates an identifier by analyzing 10 different regions of randomly repeating DNA sequences (Short Tandem Repeat Sequences) that differ among individuals (Parliamentary Office of Science and Technology 2006a). Such systems are typically accessed by law enforcement agencies to identify suspects, by matching crime scene DNA samples to those in the database. The DNA database can be considered an extreme form of identity management. For example, DNA identification has become a highly deterministic in that judgements are made solely on DNA identification—irrespective of other evidence—even though experts warn of the dangers this harbours (2009). The system contains not only the DNA of convicted criminals, but of all suspects, and persons who gave DNA for purposes of being eliminated from an investigation. There has been a public debate on the way in which the system is operated, and legal challenges which resulted in a recent ruling that the system violates *Article 8* of the European Convention of Human Rights (BBC 2008b).

The second identity system covers digital identities in an online environment. Austria is regarded as a leading implementer of e-government among the European countries. To facilitate its vision for the provision of online services, the government concluded that it required a system to support the identification and interaction of services in a digital environment. The concept of the Austrian Citizen Card was defined to fill this role (Leitold and Posch 2004). Even though the name 'Citizen Card' suggests otherwise, it is not a single physical card—rather, it is a concept for a set of standards and requirements that have been developed to support digital identification and authentication (Arora 2008). The Citizen Card outlines mechanisms for secure digital identity and digital signatures. Individuals can obtain Citizen Cards from a number of providers. For example, digital signatures are automatically loaded onto official government eCards, where individuals will need to voluntarily activate the digital signatures in order to use it. Alternatively, individuals can choose to load and activate the digital signatures onto Bank ATM cards and even mobile phones (Meints and Hansen 2006).

Rollout of the Austrian Citizen Cards to the entire population was completed by the end of 2005, but by early 2009, only 74,000 individuals had activated their digital identities and signatures (Martens 2010). This represents 0.9% of the overall Austrian population, with a very slight increase of about 0.2% from the year ending 2005 (Meints and Hansen 2006). A-Trust, an Austrian certification service provider, attributes the lack of adoption to the complexity, cost and lack of benefit from an individual's point of view (Sokolov 2006a, b).

Structural properties

This section introduces the structural properties of the framework. Each individual property will be applied to the UK DNA Database and the Austrian Citizen Card contexts (see "Privacy"). The structure of an identity system refers to the manner in which an identity ecosystem is constructed—these are key choices system owners and designers can make about the identity system, which directly impact an individual's lived experience. These properties seek to capture the flow of information inside the web of identity that is established. The structure of an identity scheme will define how the interaction between individual and society is shaped by the identification system, affecting the possible outcomes that an individual will face.

Control Points

One of the main structural properties of any identity system can be expressed in terms of the number of *Control Points*, which represents the situations in which an individual's identity is required in order to proceed with a particular function. This includes situations where identity and personal information are being consumed for the purpose of identification and authorisation, as well as situations where the information is being captured for the purpose of enrolment or updating. A simple example would be the need to show proof of age when purchasing alcohol. Without the proof, the individual would not be able to proceed with the purchase. When an identity ecosystem contains a large number of *Control Points,* the identity is frequently accessed by the relying party. A low number of *Control Points* implies that an individual's identity is not used or requested frequently.

In the context of the DNA Database, each time a DNA sample is extracted from a crime scene or taken from an individual it is checked against every single identity entry in the database. According to the official statistics (National Policing Improvement Agency 2010) in 2008/09, a total of 14,452 crime scene samples have produced a match from the DNA database, with a total of 410,589 matches since 1998. This means that every single identity within the system has been accessed, at the very least, 14,452 times in 2008/2009—a high number of *Control Points*. In contrast, the Austrian Citizen Card system is designed as a voluntary system to support eGovernment services. However, the average number of interactions between individuals and the public sector has been roughly estimated to be "*1.7 contacts per year*" (Aichholzer and Strauß 2010). This represents a low number of *Control Points*. Furthermore, for a majority of these online services can be accessed without the use of an Austrian Citizen Card (Aichholzer and Strauß 2010). As the Citizen Card does not have to be used in these contexts, they are not true *Control Points*, further reducing this number.

How does the number of *Control Points* affect the *lived experience*? A high or low number of *Control Points* in itself is not positive or negative. A high number of *Control Points* in the DNA database implies that an individual's identity is constantly being accessed. This means the DNA Database becomes a surveillance tool that authorities use to deter individuals in the database from committing crimes (2007; Science and Public Protection 2009). Situations where individuals are "constantly watched" can create feelings of paranoia, which can limit individual freedom. The low number of *Control Points* in the Austrian system indicates a lack of opportunity to make use of the identity, creating perceptions that there is little benefit in using the system (Aichholzer and Strauß 2010).

Subject Engagement

This property captures whether an individual is an active or passive participant in the use of the identity. A system with a high level of Engagement gives individuals an active role in the presentation of their identity, usually meaning an individual needs to be present, or is at least aware, when their identity is used. On the other end of the spectrum, individuals can be completely passive members of an identity scheme. Systems with a centralized database that stores information usually have low levels of *Subject Engagement*, as records stored on the database can be accessed by the organisation without the individual being present, and be unaware that the identity is being accessed.

Forensic criminal identification systems—by their nature—do not directly involve individuals, because there is an assumption that criminals will attempt to evade authorities if they are aware that they have been identified as suspects of a crime. The DNA database is no exception; an individual is only involved during the initial DNA collection, and following positive identification. Any other access of the information happens without the individual's involvement or knowledge. Therefore, as an individual assumes a very passive role, the DNA database has a low degree of *Subject Engagement*. In contrast, the Austrian Citizen Card is a voluntary system that requires individuals to take initiative in the activation and use of their digital signature (Aichholzer and Strauß 2010). It has a high degree of *Subject Engagement*.

If there is a low level of *Subject Engagement,* individuals may not be aware when their identity is being used. This can create concerns about who might be accessing the identity, what they may be doing with the information and the consequences this might have for the individual. In the case of the DNA Database, DNA profiles have been handed out to private firms for research purposes, such as the development of familial searching (identifying relatives through DNA), without the respective individual's knowledge (Hope 2008). A high level of *Subject Engagement* minimises this risk for privacy invasions, but introduces the possibility of the system becoming an unacceptable burden for an individual, as he or she is now required to exert effort to make use of the identity. The activation process for the Austrian Citizen Cards is cumbersome. The actual usage of the digital signatures has a high learning curve, and problems can still occur during use (Aichholzer and Strauß 2010). Therefore, the system requires a large amount of effort in relation to the potential benefits, helping to explain the resistance in the form of non-adoption of the system.

Identity Exposure

An individual is typically enrolled into an identity system to determine his/her respective rights, privileges and/or the necessary course of action—this involves the presentation and use of individual identities at various *Control Points*. The process of the identity being accessed and used by a relying party carries with it the risk of the identity being exposed to other, non-reliant parties. Uncontrolled disclosure of information can be expressed as the degree of *Identity Exposure*; it refers to the degree of control that individuals have over the presentation of his/her identity to the rest of society, highlighting issues around social perceptions, values and acceptance of such identities. A system with a high degree of exposure constantly reveals the identity information to third parties that have no rights or permission to obtaining the identity. Identity systems that allow an individual to preserve the integrity of the identity from other parties have a low degree of *Identity Exposure*.

In the case of the DNA database, individuals have no control over the presentation of their ("criminal") identity to the rest of society. This is especially true in connection with serious crimes, where a positive DNA match is seen as an indication of guilt, and can trigger a man-hunt via media channels. The Austrian Citizen Card has been designed as an identification and authentication mechanism, and therefore does not provide the identity of the individual to anyone but the relying parties the individual is interacting with. The use of sectoral identifiers—which are unique identification numbers that differ within different contexts of use—further protects individuals from exposure; there are 26 sectors (such as tax, health, education, etc.) that each use a different identifier per individual. This prevents the connection of different identities across separate contexts (Aichholzer and Strauß 2010).

A high degree of *Identity Exposure* potentially means an individual cannot evade judgement by third parties based on the revealed identity. Shortly after the European Court ruling on the database being a "*breach of rights*" (BBC 2008b), a police chief at the time defended the database stating that *"the public expectation now is that crime will be solved, not by the presence of witnesses, but because there will be DNA..."* (O'Neill 2008). Although not a directly associated with the UK DNA Database, the events following the disappearance of Madeline McCann in Portugal illustrate public perceptions of the connotations of a DNA match. When Madeline's DNA was found in the boot of the car that her parents had hired, initial sympathy over the disappearance of their daughter quickly turned to "*defamatory comments*" because the presence of DNA was seen as proof of their involvement in her disappearance (The Independent 2007). A low degree of *Identity Exposure* means there is a low risk of uncontrolled exposure of an individual's identity. In the Austrian Citizen Card Scheme, an individual's digital identity and signature is loaded onto his/her personal device, such as the government eCard. The device and therefore, the identity is under the individual's control ensuring that the identity doesn't leak out without the individuals knowledge (Leitold et al. 2002). Furthermore, the use of the identity takes place in a digital medium that makes use of encryption and secure digital channels for communication. This provides the system with a low degree of *Identity Exposure* ensuring that the individual remains in control of the identity.

Population Coverage

Population Coverage describes the number of individuals that are registered in and interact with the system, in relation to the size of the total population (which are not enrolled in the system, but are still able to act in the context of which the identity system operates). A system with a low level of *Population Coverage* would be highly targeted—the number of individuals that are registered on the system consists of a small part of the entire population that are able to act in that context. On the other hand, a system where all or most individuals are automatically enrolled has a high level of population participation.

While the UK DNA database is currently the world's largest DNA database, it holds about 4.8 million individual DNA samples; representing only 7.39% of the total UK population (Hayles 2009). This implies a low level of *Population Coverage*, i.e. a highly targeted form of identification. In contrast, the Austrian Citizen Card system was designed as a universal identity scheme. Given that the eCards has been distributed to the entire population, it has a high level of *Population Coverage*.

Low levels of *Population Coverage* can be linked to issues of discrimination. Individuals are identified simply by being part of the system—and are more likely to be unfairly scrutinised by authorities in comparison to those who are not. In its review of the UK DNA Database, the European Court of Human Rights has ruled the retention of the DNA of un-convicted individuals as unlawful (BBC 2008b). Significantly, the inventor of DNA fingerprinting, Sir Alec Jeffreys, has called for DNA of non-convicted individuals to be removed stating that "*there is a presumption not of innocence but future guilt*" (Whitehead 2009). There are also systematic biases in terms of population selection—the DNA of 40% of young black males is in this database—which led a judge to suggest that all citizens' DNA should be captured (Orr 2007; BBC 2007a). The Austrian Citizen Card has a high level of *Population Coverage*. The universality of the system over the entire population, removes the possibility of distinctions being made against those who are enrolled against those without an identity. Therefore the issue of possible discrimination based on the enrolment into the Citizen Card scheme has been eliminated.

Metrical properties

This section introduces the metrical properties that were coded in the thematic analysis. Each metrical property will also be discussed within the context of the UK DNA database and the Austrian Citizen Card (see "Privacy"). The metric of an identity system refers to the techniques, methods and technologies that are used to capture and present an individual's identity. The metrical properties defined here capture the implication that the type of information has on the lived experience of the individual.

Expert Interpretation

The first metrical property is the level of *Expert Interpretation*, which captures the amount of human activity required to collect and use identity information. Systems with a high level of expertise require specially trained staff to handle the identifying metric at various stages throughout the lifecycle of the identity. Systems that require a high level of *Expert Interpretation*, as opposed to systems where anyone can interpret the identifiers, involves subjective judgements, where the determination of identity depends on the examination of information by human experts. Automated systems serve to decrease the amount of expert analysis involved, providing systems with an objective approach to processing identity.

DNA identification works by matching specific DNA markers obtained from two separate samples (Parliamentary Office of Science and Technology 2006b). If the two samples contain all of the same markers, a match is made (positive identification). Specific equipments are required as part of this process, but it is not an automated one, as several steps require interpretation to determine if there is a match. The decisions to ignore, accept or to reason about the absence or presence of certain markers brings a degree of subjectivity into the identification process, creating a system with a high degree of *Expert Interpretation*. On the other hand, digital signatures are built on mathematical models of encryption, offering an implementation that is completely objective and automated. The process of identification does not require human beings to interpret an individuals identifying or authenticating information. Therefore, the Austrian Citizen Card system has a low degree of *Expert Interpretation*.

A high degree of *Expert Interpretation* implies a reliance on subjective decisions about an individual. It creates a non-transparent situation, where non-experts cannot assess the reliability of the identification process, leading to an assumed infallibility of the expert decisions. This leads to the possible implication that an individual can be wrongly identified, and in the case of a criminal system he/she might be wrongly accused of a crime. The 1993 case of Timothy Durham in Oklahoma (W. C Thompson et al. 2003) illustrates the potential consequences of such mistakes. Timothy Durham was found guilty of raping an 11 year old girl, based on the alleged victim's eyewitness identification, a hair sample from the scene that was similar to Durham's hair, and most importantly the DNA test of semen—which matched Durham. The guilty verdict was passed despite 11 witnesses placing Durham in Dallas at the time of the rape. Durham was eventually set free in 1996, after further testing revealed that the semen could not have come from him and highlighted the error in the initial DNA test that *"arose from misinterpretation"* (W. C Thompson et al. 2003). A low degree of *Expert Interpretation,* such as the Austrian Citizen Card, eliminates the risk and the dangers of subjectivity as the identification process is an objective process free of human error. Objectivity creates a predictable process that provides a level of transparency in assessing the correctness of identifications.

Population Comprehension

Another metrical property is the general level of understanding that the population at large has of the techniques and technologies used for identification. In a system with a low level of *Population Comprehension*, citizens have little to no knowledge on how the metrics are used to identify them. This typically happens when a large number of the general population cannot interpret the significance of an identification being made, why it may be wrong, or how the identity system works. On the other hand, systems with high levels of understanding are those in which an individual has a good mental representation of the entire process in which the identity metrics are used.

Whilst there is a high level of awareness that DNA is used for identification, most individuals do not understand the process by which identifications are made, nor can they easily grasp the implications behind the probabilities attached to DNA matching—such as a "*one in trillions*" probability of a chance match occurring between two unrelated individuals (E. Graham 2007). A recent study (Ley et al. 2010) found that perceptions of the entire DNA process have been shaped by a "*CSI effect*", in which the inaccurate media portrayal of DNA applications has distorted perceptions of the entire identification process. As such, the DNA database has a low level of *Population Comprehension*. Similarly, the Austrian Citizen Card also suffers from a low level of *Population Comprehension*. Digital Signatures are not a technology that is easily understood by laymen (Garfinkel et al. 2005a). A study of merchants trading through Amazon (Garfinkel et al. 2005b) found that only 54% of those understood how the digitally signed receipts they were receiving worked. 59% of merchants thought it was important to use encrypted and signed mail, yet 59% also admitted to not knowing whether their eMail client supported it.

Low levels of *Population Comprehension* indicates the possibility that individuals cannot challenge identification decisions, as people in general do not understand how the information is processed, nor do they know how to interpret related figures. In the case of Madeleine McCann (see "*Identity Exposure*"), traces of her DNA was found in the boot of the car hired by her parents. For many people reading this in the press, and members of the Portuguese police, the presence of Madeleine's DNA implicated her parents (Rayner et al. 2008). However, DNA can be easily transferred via her clothes and toys that had been transported in the boot. Another issue brought by low levels of *Population Comprehension* arises in voluntary use systems. If individuals do not understand how to use the identification technologies, such as digital signatures, they may not be able to identify themselves when they need to, and/or be fooled by fake credentials. In this context, the low levels of *Population Comprehension* can indicate potential confusion on how to make use of the identity and therefore the system. This can be linked to the issue of complexity that has been raised in the Austria Citizen Card scenario, contributing to the situation where individuals are not using the digital signatures resulting in low rates of adoption (Sokolov 2006a, b).

Information Accuracy

Information Accuracy is the property that defines the reliability of the information that is collected, stored and used in the identity system. Systems with high degrees of *Information Accuracy* are more likely to produce correct identifications. However, this accuracy must not be based solely on the theoretical possibilities—accurate "measurement" of *Information Accuracy* needs to take into account the implementation specific details that can affect the theoretical probability. The inconsistencies and practical limitations of the real world will need to be reflected in the *Information Accuracy* property of the system.

DNA identification can offer high degrees of accuracy if the samples being compared are of high quality (Graham 2007). In law enforcement, however, DNA samples are not only collected from individuals, but also from the crime scenes. Such samples may be contaminated by other DNA present at the scene, or might have degraded over a period of time before it is captured and stored. Although it is difficult to measure the effects of contamination or degradation, it is important to note that this decrease in the degree of *Information Accuracy* reduces the probability of a correct identification being made (Thompson et al. 2003). Austria's Citizen Card scheme offers a high degree of *Information Accuracy.* The system is designed around unique identification numbers and digital signatures that are issued to each individual in the population (Leitold et al. 2002). If implemented correctly, the use of digital signatures should leave no doubt as to its authenticity.

The impact of a low degree of *Information Accuracy* on the lived experience is that individuals are at risk of false positives (falsely matching someone to a DNA sample), resulting in individuals being wrongly accused. In the recent case of the Omagh bombing, the judge called into question the reliability of the Low Copy Number (LCN) DNA identification technique, which makes use of minute DNA samples for matching purposes (2007). The merit of the technique is still being debated in the scientific community (Graham 2008). As a result of the case, the police suspended the use of the LCN technique, which up to that point had already been used in 21,000 different cases (Hope 2007). In the case of Timothy Durham see "*Expert Interpretation*". (Thompson et al. 2003), the misinterpretation of the DNA was a result of the failed separation of the contamination between the male and female DNA during extraction of the semen stain. When an individual first activates an Austrian Citizen Card, an "*identity link*" is created based on unique citizen identification (H. Leitold et al. 2002). The identity link also contains name, date of birth, and an individual's public key that is used to support digital signature functions. This identity link is then digitally signed by a government authority, which prevents tampering, and provides high levels of assurance that the identification information held on the card is accurate—minimizing the danger of erroneous identification of an individual caused by inaccurate information.

Information Stability

The chosen metric for an identification system will also have an impact on the stability of the registered identity. *Information Stability* refers to the rate with which the information stored in an identity system changes over time, and thus supports reliable identification—long after it was first recorded. A system with low *Information Stability* means the identity information has the potential to fluctuate greatly over short time frames. Identity systems that make a large use of biographical information typically have low levels of stability as the information can potentially change at any given time (e.g. address, profession, etc.). Some biometrics can seem to be stable over the lifetime of an individual (e.g. iris), whereas others change over time, or can be altered by the individual (e.g. face recognition).

An individual's genetic makeup does not change over time, and offers a high degree of "*permanence*" (Jain et al. 1999). This means that regardless of the time between collection and identification, an individual's DNA sample will always produce a match with that particular individual. As such, the DNA database offers a high level of *Information Stability*. The information used to establish an individual's identity in the Austrian Citizen Card scheme (i.e. identification number, name, date of birth and public key) does not tend to fluctuate greatly over time. For example, an individual cannot change his/her date of birth, and is usually tied to a single identification number over a lifetime. Therefore, the Austrian Citizen Card has a high level of *Information Stability*.

A high level of *Information Stability* potentially threatens individual freedom, as an individual is unable to redefine his/her personal identity to evade detection if the DNA is used for different purposes. Austrian Citizen Cards also have a high level of *Information Stability*, and are subject to the same potential issues. Even though an individual can change his/her name or be issued with a new public key, the unique identification number and the centralization of such change processes allows the government to maintain a link of the "new" identity to the original identity that was first created.

Subject Coupling

Identification systems do not only vary in terms of the stability of the information collected, but the amount of information that is collected and used for a particular purpose. This property of the system is known as *Subject Coupling*, i.e. the degree of representativeness between the captured identity and the relevant "*partial identity*" (Pfitzmann and Hansen 2008) of the individual in relation to the purpose and context. A tight coupling suggests that the captured identity metrics faithfully represents an individual's partial identity at the various *Control Points* that it is applied. On the other hand, a system that collects too much or too little information about an individual is said to have a low *Subject Coupling*, since the identity that is captured and presented does not accurately represent the 'complete' individual in that situation. While this property may seem like an easy aspect to establish, ensuring that *Subject Coupling* is accurately assessed depends on more subtle nuances about the information around the identity and the context.

While a lack of information to represent an individual means that there is a low *Subject Coupling*, the inverse is not always true. *Subject Coupling* occurs when the identity created does not represent the individual in the context. Collecting 'too much' information also results in low levels of *Subject Coupling*. When too much information is known about an individual, the consumer of that identity might then judge the individual based on information that is not relevant for the particular purpose (Fig. 2). An example of having too much information would be the use of branding to enable authorities to identify recidivists (Caplan and Torpey 2001). When released, the physical marks were clearly visible to everyone, all the time. This removed any chance of re-integration into society.

Consideration of this property requires designers and implementers to account for an individual's own perception of the relevant partial identity. As such this property should not only be considered from the organisations point of view, but must also consider how each individual perceives their role with respect to the organisation. The focus is on the relationship between the individual and the implementer, influencing the information that the individual assumes is relevant to the instantiated identity. Therefore, *Subject Coupling* must also ensure that there is a good mapping between the individual's perception of the relevant identity and the organisation's perspective of the relevant identity.

The DNA database is meant to identify people connected to crime—either to pursue further investigation, or to eliminate a potential suspect from it. If the identity is limited to just the elimination of suspects, the system would have a high degree of *Subject Coupling*. However, the faith that many individuals put into such systems means DNA has become a highly deterministic form of identification: a positive DNA match can greatly influence the perception of an individual's identity, causing other relevant information to be discarded or distorted in light of the match. Furthermore, in relation to keeping DNA of non-convicted individuals, a recent report from the Home Office (Science and Public Protection 2009 has stated that the "*risk of offending following an arrest which did not lead to a conviction is similar to the risk of reoffending following conviction.*" This can be interpreted as an assumption of guilt through association with the DNA database, where the view becomes that "*innocent people who have been arrested are more likely to commit a crime*" (Goldacre 2009). The system can therefore be said to posses a low level of *Subject Coupling.* The Austrian Citizen Card system is designed as a digital identification and authentication scheme. Its purpose is to provide individuals with mechanisms to securely and accurately identify themselves to other organisations.

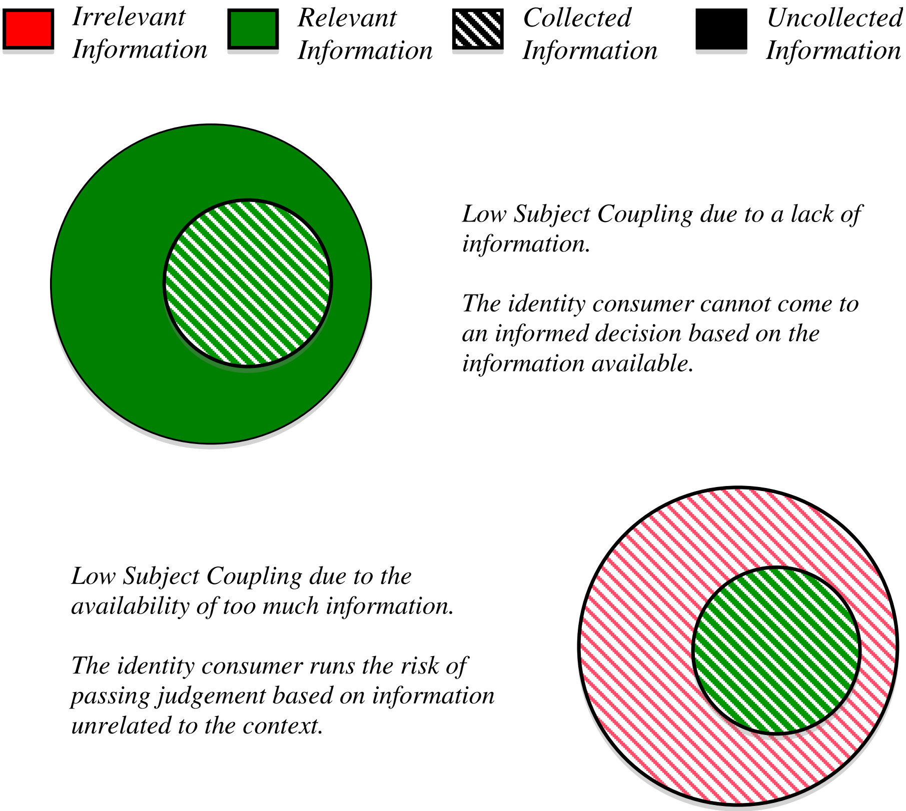
Irrelevant Information
Relevant Information
Collected Information
Uncollected Information
Low Subject Coupling due to a lack of information.
The identity consumer cannot come to an informed decision based on the information available.
Low Subject Coupling due to the availability of too much information.
The identity consumer runs the risk of passing judgement based on information unrelated to the context.

Fig. 2 Low levels of *Subject Coupling*

Therefore, the identity link created, based on the unique id number, the name, the date of birth and public key (H. Leitold et al. 2002), seems to fit its purpose and does not collect or make use of other information beyond what is needed. It provides a high level of *Subject Coupling*.

A low level of *Subject Coupling* indicates the potential dangers where individuals may be judged on an unrepresentative form of identity. Raymond Easton was charged with burglary when his DNA sample was matched to a crime scene (BBC 2007b). However, Mr Easton was in advanced stages of Parkinson disease, and could not have committed the crime. While he was eventually released and the charges dropped, this only came after an advanced DNA test was made. In a separate case from 1997, George Ellis was sentenced to 14 years in prison for robbery (BBC, 1999) Despite claims that it was planted, he was convicted solely on the DNA evidence. Two years later, criminal charges were brought against detectives involved in George Ellis's case, calling into question the validity of the DNA evidence. An appeal court came to the conclusion that it could not uphold the conviction since the "*DNA evidence was the most damning piece against him*" (1999). As such, having a low level of *Subject Coupling,* the DNA database introduces situation where decisions to be made based solely on the positive DNA match. Offering a high level of *Subject Coupling*, individuals in the Austrian Citizen Card system are not unfairly judged based on the identity created. The information used in the scheme is sufficient just for purpose of identification. Its use in different contexts (health, tax, etc.) will then be supplemented with other personal information that will need to be collected and stored by each relying party, whose information systems remain independent of the Citizen Card system (H. Leitold et al. 2002).

Information Polymorphism

Depending on the chosen metric, an individual's identity may be more or less likely to being used for different purposes. The likelihood that the identity may be used for a different purpose increases with the various meanings that can be attributed, extracted or interpreted from the type of information held about individuals. This is captured by the term *Information Polymorphism*. This property is derived from the quality of the information itself, and therefore needs to be assessed irrespective of any laws that are put in place to prevent such abuse of the collected information. Such safeguards are easily circumvented, especially if the required information has already been collected and stored. In systems with a high level of *Information Polymorphism*, an individual's identity information can be easily taken out of context of the original scheme, and applied to other systems that use this information for different purposes. Such systems are more likely to lead to what is commonly described as *function-creep*. A low degree of *Information Polymorphism* means that an individual's identity is safe from being exploited for other functions.

DNA can be used not only for individual identification purposes, but also for a number of other purposes such as identifying racial heritage and familial linkages (paternity), or the likelihood of developing certain illnesses. The DNA database therefore has a high level of *Information Polymorphism* since information can potentially be used for completely different purposes. The identity created in the Austrian Citizen Card system relies on information that does not lend itself to various uses. For example, the public key can only be used to support authentication or digital signing procedures. Furthermore, each service that an individual interacts with will make use of different sectoral identifiers preventing the combination of information across various contexts (Meints and Hansen 2006), reducing the possibility of information being joined together for other purposes. The Austrian Citizen Cards therefore offers a low level of *Information Polymorphism*.

A high level of *Information Polymorphism* potentially threatens individuals' privacy. The DNA stored in the UK DNA database is currently governed by law that states it can only be used to investigate crime. However, the Chief Constable in charge of the database regularly receives requests for matching to be performed for paternity cases; even though these are refused, the risk of paternity suits has been cited as a reason why police officers do not want their DNA to be stored for elimination purposes (Bennetto 2000)—something that is done with fingerprints. Furthermore, there is the issue of unpredictable future governments and how they might potentially change laws around the collection and use of DNA information. For example, when the DNA Database was first implemented in 1995, the law stated that only the DNA of convicted individuals would be stored in the Database. This was later changed when the Criminal Justice and Police Act 2001 allowed the government to collect and store DNA of non-convicted individuals.

At first glance, the use of unique identification numbers in the Austrian Citizen Cards might imply a high level of *Information Polymorphism*, as these identification numbers typically allow for the linkage of information across different contexts of use. Unique identification numbers allows for the creation of detailed user profiles that can invade an individual's privacy. For example, (Lyon 2003) mentions how insurance companies in the United State use increasingly intrusive methods to collect personal information based on an individual's Social Security Number. The Austrian Citizen Card has been designed to minimise risk, by creating unique sectoral numbers. In a particular context of interaction, the unique identification number goes through an irreversible cryptographic hash to produce a new sectoral identification number that is then be used to identify the individual within that particular context (H. Leitold et al. 2002). This prevents an individual's identity from being linked up across different contexts, containing an individual's information to use within each scenario. This creates a low level of *Information Polymorphism*, minimising the possibility of privacy invasions and function creep.

Combining properties

Looking at the various properties individually—as we have in the preceding sections—can help researchers and practitioners to understand the possible impact of an identity system on the lived experience. In certain configurations, such as an identity system a high number of *Control Points*, the system might be perceived as being—'too controlling', and would thus might be met with resistance. A system that needs to be up-to-date, but makes use of a metric that has a low level of *Identity Stability,* may be seen as a burden upon individuals, who continuously have to report when information changes.

However, reactions to identity systems are rarely brought about by any single property alone. It is the combination of these various properties and their interactions that allows for the proper assessment of the lived experience. In doing so, one can then construct the possible narratives and therefore the potential outcomes while paying attention to the various contextual elements and social norms. For example, consider a system with a low level of *Population Coverage*, a high level of *Subject Engagement*, and a high number of *Control Points*. The resulting identity system is a highly targeted one, indicating that certain criterion needs to be met for inclusion into the system. The majority of the population that is acting in that particular context is able to bypass the system. Additionally, as individuals play an active role at a large number of *Control Points*, some might decide that the burden of the system is unbearable. As such, in cases where it is possible to do so (e.g. identification systems based on religion), one can analyse the situation and deduce that a number of individuals might avoid the identity system altogether, by abandoning his/her 'identity' and constructing a new one.

With the Austrian Citizen Card, there was lack of adoption and use of the digital signatures (Sokolov 2006a, b). Putting the system in the context of the properties, we can link the low uptake of the system to the low benefit for individuals, as there are few instances where they can make use of their identity (low number of *Control Points*), and the fact that digital signatures are not understood by many people (low levels of understanding), As such, being individuals that play an active role (high level of *Subject Engagement*), they are not motivated to make use of their digital signatures.

For the DNA database, most of the properties introduced here are relevant to interpreting the various reactions towards the system. The initial set of privacy concerns stem from the constant access of the identity (high number of *Control Points*) of which the individual is unaware (low levels of *Subject Engagement*). This is further amplified by the possibility that the identity information can be easily reused for other purposes in completely different contexts (high level of *Information Polymorphism*), again potentially without the individual being aware.

Issues of fairness and freedom also come into play when considering the highly targeted nature of the DNA database (low level of *Population Coverage*), especially in light for the lack of control that an individual has over the presentation of the identity to the rest of society (high level of *Identity Exposure*). Furthermore, the lack of control is substantially worsened by the incomplete yet deterministic nature of such identification (low degree of *Subject Coupling*), that takes places in a subjective process (high levels of *Expert Interpretation*) based on potentially inaccurate information due to contamination and degradation (low levels of *Information Accuracy*).

Based on this narrative for the DNA database, it is not surprising that the system is surrounded by privacy concerns and controversy. These concerns are given strength, perhaps non-intuitively, by the broadening of the *Population Coverage* as it includes not only convicted criminals but suspects as well. This can perhaps be explained by the fact that it is still a highly targeted system, just slightly broader in scope, Additionally, from the point of view of innocent suspects, they do not belong on the database at all, meaning the partial identity created goes against the relationship between the individual and the state, thus further driving down the level of *Subject Coupling*.

Applying framework to non-government identity systems

The system properties introduced in this paper were developed through an investigation of past and present National Identity Systems, and we have explained them in the context of two such schemes. To illustrate the applicability of the properties to different contexts, the properties will be used to investigate identity and information systems that have been implemented in completely different environments. In the following, we apply the properties to a social networking system, and a personalized advertising platform.

Social networking

Online Social Network Sites (SNS) have experienced significant growth over the past few years. It has become an increasingly popular medium for individuals to connect with each other and share a high degree of personal information. From our point of view, an SNS can be viewed as an Identity Management System. This makes such sites a prime candidate by which we can apply the codes that the research has uncovered. Specifically, we will be looking at the Facebook platform.

With over 200 million registered individuals, Facebook is arguably the most popular social platform today. It has also been the centre of some controversies. Just recently Facebook has been accused of breaching Canada's Privacy Laws (BBC

Table 4 A brief analysis of systems used in thematic coding

System	Structural Properties				Metrical Properties					
	Control Points	Subject Engagement	Identity Exposure	Population Coverage	Subject Coupling	Population Comprehension	Expert Interpretation	Data Accuracy	Data Stability	Data Polymorphism
Poor Law Badges	***High***	***High***	***High***	***Low***	***Low***	*High*	*Low*	*Medium*	*Low*	***High***
	Few people came forward to request for an identity. *Beggars were required to prove that they could not get work. They were required to wear badges at all times in order to prove that they have the right to request for alms.* *A small number of individuals had to constantly wear badges on their arms, which were clearly visible to everyone else. This shamed individuals, making them unwilling to come forward.* *Furthermore, the information was also to determine parenting ability, a purpose that differs from the original.*									
Criminal Wanted Lists	*Low*	*High*	*High*	*Low*	*High*	*High*	***Low***	***Low***	***Low***	*Low*
	High rates of evasion. *The system is based on a simple set of physical descriptions that had a focus on the attire of individuals. This data was not very accurate and involved a high degree of subjective decisions as to a match. Furthermore the individual can easily change his physical appearance by donning disguises or new attire.*									
Russian Internal Passports	*High*	*High*	*Low*	*High*	***Low***	*High*	*Low*	*Low*	*High*	*Low*
	Large number of evasion attempts and manhunts were frequently launched. *The identities created tied individuals to a piece of land where they were required to work. This identity was rejected by individuals who did not agree with the relationship and attempted to flee from the state.*									
French 1912 Law	***High***	***High***	*Medium*	***Low***	*Low*	*High*	*Low*	*Medium*	***Low***	*High*
	Part of the targeted population (Romani) abandoned their way of life and assumed new identities. *The system was a burden on individuals, constantly showing their identities when ever they moved. Being a highly targeted system, an individual can avoid the system by "changing" his/her identity.*									
French Bertillonage	*Low*	***High***	*Low*	*Low*	*High*	*Medium*	***High***	***Low***	***Low***	*Low*
	Reliability and effectiveness of recidivists was called into question. *The identification process was highly subjective using inaccurate information, resulting in inconsistent identifications. As individuals were involved in the identification process, they could alter their dimensions by not fully co-operating, e.g. not standing straight, etc. Furthermore, it was ineffective at identifying young individuals as they were still growing.* *In Argentina, system was rejected on grounds that the measurements insulted their honour. It can be argued that they either did not understand the process or they felt that it was a misrepresentation of their identity.*									

System	Structural Properties				Metrical Properties					
	Control Points	Subject Engagement	Identity Exposure	Population Coverage	Subject Coupling	Population Comprehension	Expert Interpretation	Data Accuracy	Data Stability	Data Polymorphism
Argentina Dactyloscopy	*Low*	*Low*	*Medium*	*Low*	*Medium*	***Low***	***High***	***Medium***	***High***	*Low*
	Dactyloscopy has become a de facto standard in criminal investigations. *Fingerprints collected did not change over time and was more accurate than body measurements or descriptions. It gave the identification of criminals a form of "mechanical objectivity" in that the fingerprints were captured using objective approach.* ***Issues of false accusations have recently been called into question.*** *Dactyloscopy still requires subjective decisions to decide if there is a match. Crime scene fingerprints are not accurate representations of fingerprints, further raising the error rate. People are not aware of the entire fingerprint identification process and therefore individuals lose the ability to resist such accusations.*									
WW I and II UK Identity Cards	***High***	***High***	*Low*	*High*	***Low***	*High*	*Low*	*Medium*	***Low***	*High*
	Individual information was out of date. *The information collected included attributes such as address which were open to change. The high variability in the information collected and stored, required the co-operation of individuals to update their records as needed. The public however proved unwilling to assist the in these procedures, especially since the cards did not provide any benefits after war time (after its use in food rationing). It is perceived as the needless prussianzing of institutions.* ***Resistance to carrying and showing ID Cards.*** *The needs for identity cards represent a clash in the culture for the public. The identity created by such a system goes against the relationship that exists between the state and its people. Therefore, the identity instantiation did not match well to the individuals' perception of the situation. This led to resistance towards hosing ID cards, as in the case of Wilcock, which was brought to court and gained a lot of public support and negative media publicity against the ID cards.*									
WW II Nazi Jewish Identity System	***High***	*High*	***High***	***Low***	***Low***	*High*	*Low*	*High*	*High*	***High***
	Paralysis of the Jewish Population. *The identity system created was highly targeted to the Jewish population. It started of as an identity document with clearly stated markings, indicating the individual was a Jew. This eventually led to the use of symbols that had to worn and be visible at all times. This made the Jewish directly visible to the other members of the population limiting their freedom and movements* ***Aid in the mass killings.*** *The biographical information used in the system, lends itself to other purposes. In this particular case, it made it easy to gather and round up the Jewish population aiding in the act of genocide.*									

Table 4 (continued)

System	Structural Properties				Metrical Properties					
	Control Points	Subject Engagement	Identity Exposure	Population Coverage	Subject Coupling	Population Comprehension	Expert Interpretation	Data Accuracy	Data Stability	Data Polymorphism
UK DNA Database	***High***	***Low***	***High***	***Low***	***Low***	***Low***	***High***	***Medium***	***High***	***High***
	Large amount of privacy concerns have been raised. *The DNA is information constantly being accessed without individuals being aware of it. Furthermore it is a highly targeted system that also includes non-convicted individuals. These individuals do not believe they should be on the database, crating a situation of conflict in the creation of the identity. This becomes a major concern since individuals cannot control the presentation of identity to the rest of society.*									
Contact Point	***High***	*Low*	*Medium*	*High*	***Low***	*High*	***High***	***Low***	***Low***	*High*
	Effectiveness of system has been called into question. *Recent cases, such as the death of "Baby P.", have raised doubts on the usefulness of the system. The individual's information being entered into the system is not objective and reduces the accuracy of the data collected. Furthermore, interpretation of results is highly subjective. As the "Babpy P." case shows carers were all aware of each other, but still failed to recognize the trail of abuse.* ***Issues of freedom and self fulfilling prophecies have been raised.*** *Services that make use of the information may pre-emptively judge an individual and change their modes of interaction. The individual is potentially being assessed on an incomplete picture of his/her identity based on interactions from another context. Furthermore, being targeted at children, such information is not stable and will continuously change, reducing the representativeness of the individual's identity.*									
Austrian Citizen Card	***Low***	***High***	*Low*	*High*	*High*	***Low***	*Low*	*High*	*High*	*Low*
	Low rates of adoption in the digital signature functionality of the Citizen Card. *The system does not present an individual with many opportunities to make use of the identity, creating a lack of perceived benefits. Furthermore, individuals do not understand the system making it difficult to use.*									

News 2009). More relevant to our considerations is a change that Facebook made to its website that brought out negative reactions among its community.

In 2005, Facebook introduced new features that affected the way in which information was distributed to an individual's network on the site. Prior to these changes, information that was inserted or updated on an individuals profile was only visible when another party visited his/her profile page. Facebook then added the *Newsfeed* feature, which essentially aggregated all these information changes and broadcast them to an individual's friends. This turned a process from a 'pull' operation to a 'push'. Individuals reacted against this and established resistance groups to voice their opinions. The Facebook CEO eventually responded, stating that no privacy options were taken away, and that the information was visible only to the same people who has access as before. "*Nothing you do is being broadcast; rather it is being shared with people who care about what you do*" (Hoadley et al. 2009). Nevertheless, Facebook took down the Newsfeed, and re-released it with various privacy controls.

In their study of the situation, (Hoadley et al. 2009) attributed the resistance to individuals' perception of "*information access*" and "*illusion of control*". Individuals viewed the Newsfeed as increasing the ease with which their information can be accessed by others, and the absence of controls reduced the perceived level of control that individuals had. While this point of view is certainly justified, the properties that have been uncovered here might be able to shed more light on the situation and better relate the changes in the system to the reactions.

The most relevant properties for this scenario are the *Control Points* and *Subject Engagement*. Pre-Newsfeed, information was only accessible when the individual's page was visited by another party. One can technically view this as a single *Control Point*. Post-Newsfeed, the number of *Control Points* increased dramatically; every party that the information was pushed to represents a Control Point, where the individual's information is consumed.

In addition, the Newsfeed can be interpreted as a reduction in the level of subject involvement. In the 'pull' model, visiting an individual's page was a requirement. The page is a representation of the individual on the platform, whom has spent time to create a profile that represents him/her to others. Therefore, accessing the individual's profile page can be seen as a *Control Point* that has a high level of *Subject Engagement*. The Newsfeed represents a loss of involvement, as the information is taken from the individual's controlled profile and broadcast to the other *Control Points* that individuals are not aware of or have no control over.

Targeted advertising

Targeted advertising has proved to be an extremely lucrative way to increase revenues. This form of advertising involves the tracking of an individual's identity across various services. It could be something as simple as contextual targeting (using keywords based on the content of the current page), or based on individuals' browsing history across one or more sites. These browsing histories and identification details are typically handled in a decentralized manner, making use of cookies stored on the user's computer. These tracking methods have raised issues among privacy advocates.

A recent study found that a significant number of the US population object to the tracking of behaviour. Turow et al. (2005) found that 86% of young adults reject targeted advertising that tracks behaviour across different websites. Advertisers, however, say that individuals—especially the younger generation—do not mind having their habits tracked. Recent developments in targeted advertising have taken the tracking to new levels.

Phorm is a company that developed a targeted advertising platform that is tied directly to an individual's Internet Service Provider (ISP). Every subscriber to the ISP's network is enrolled into the Phorm System. Every website that an individual visits is passed through the system, and is checked against a list of advertising categories. If a match is found, the category is marked in a cookie and stored on the user's computer. This cookie is then used to provide targeted advertisement on any websites through the use of a widget. The European Union has recently proceeded with legal proceedings in light of the controversial use of Phorm (Guardian 2009). The arguments are usually tackled from a high level law based view of privacy rights. Phorm's arguments claim that people do not understand the technology and how it works, claiming that it actually provides anonymity.

Applying the structural properties from the proposed framework, the items of interest are *Subject Involvement*, *Identity Disclosure*, and the level of *Control Points*. With every website passing through the system, Phorm presents individuals with a high number of *Control Points* resulting in a very restrictive environment for the individual. This situation is exacerbated by low subject involvement at the *Control Points*. The individual's information is taken in a covert manner, without the individual being involved in the process. Phorm also provides individuals with a high level of *Identity Exposure*. The tracked information is stored on a cookie on the user's computer. In a multi-user environment, the same computer will be used by various individuals that Phorm will not be able to differentiate amongst. When serving customized ads, the system is constantly at risk of revealing an individual's preference by presenting customized content to the "wrong" individual.

From a metrical standpoint, the properties of interest are *Subject Coupling*, and *Information Stability*. Phorm is a platform used by a user's ISP to deliver targeted advertisements. The relationship between the user and the ISP is that of a consumer paying fees to gain access to the network. This relationship calls for the sharing of certain general and financial information. This is the relevant partial identity of the individual in the subscriber role. By making use of Phorm, ISP's expand beyond this boundary by tracking an individual's habits in depth. This results in low *Subject Coupling* in the ISP-subscriber relationship. Additionally, an individual's browsing habits are constantly growing and producing a very dynamic data set that results in low levels of *Information Stability*. Therefore, in order to keep an accurate representation of the individual, large volumes of up to date records are required. This raises concerns of privacy due to the tracking nature of such a system.

Discussion and conclusion

Whilst the use of modern identity management systems has increased rapidly, the understanding of what constitutes appropriate use of identity lags behind.

The disembodiment of people from transactions has increased the perceived need to capture the identity of individuals, and developments of systems have largely been driven by what is technically feasible, and the administrative convenience of the organisations that commission the systems. Whilst the rhetoric of human-centred identity has been plentiful, little research has been carried out to understand the human experience of identity in technology-mediated interactions. This paper presents a first proposal for a set of properties to understand the need of individuals when it comes to identity systems, and what constitutes acceptable use.

Strengths and weaknesses

The main strength of framework is that it fills a gap in the current approaches to identity systems, as it links design of an identity system directly to the potential lived experience. It enhances our understating of the impact of such systems on individuals, beyond the traditional views of privacy and trust. As an example, what does it mean to claim that a system invades an individual's privacy? The problem here is privacy can mean so many things; it becomes difficult to state what the exact issue is. A typical system implementer would find it difficult to link the privacy concern to the state of system itself. However, by using these properties as a support mechanism, a researcher or practioner can conduct a proper analysis of the system, communicate clearly on the potential problem areas and suggest practical design changes to reduce the privacy concern.

Another benefit of the proposed framework is that proper use of these properties encourages the designer to immerse herself in the situation that the system will be used. Proper assessment of how each property interacts with another requires thought and reflection, looking at the system from the point of view of the individual and society that is affected by it. This is a breakaway from other methods that might take a highly administration-centric point of view, or a solution that might rely on a set of checklists, that removes a system implementer from the context. The proposed properties serve to re-embed the design process into the reality of the situation in which it is implemented.

However, the subjectivity required to fully utilize the framework can also be seen as a potential weakness. While there is an element of rating taking place, one would not be able to simply assign weights of importance to each property. Each context differs from the next and each property can play a slightly different role in relation to every other property. A high level or low level of rating for each property does not automatically indicate a good or bad outcome. There is a degree of interpretation required, and different individuals might perceive things differently, which can lead to a source of inconsistent results.

Furthermore, in its current state, the predictive power of the framework remains untested. The analysis of systems using these properties has taken place post-implementation. We are fully aware of the outcomes that a particular identity system has brought about. This hindsight proves to be an advantage, as it is easier to link known outcomes to the system properties than it is to link system properties to unknown outcomes.

Further research

The human-centred framework has been developed through a grounding of previously implemented nation-wide IDMS, and has been shown to be useful in different contexts from social networking systems to personalised advertising platforms. However, it still needs to be further tested and elaborated upon. By exposing this work to the community, we hope to be able to build a robust model that can prove to be a useful tool in the quest for human-centred identity. Potential areas for further development are provided below.

The properties of the framework here have been brought about through the analysis of a specific set of identity systems. Therefore, a continuous application of these properties to other implementations can serve to discover refinements to the uncovered properties. As an example, it may be beneficial to break down the *Control Point* property into *Read-Only Control Points*, where an individual's information is only consumed, as opposed to a *Write-Only Control Point* where the individual's identity entry is updated with new information. Another possible break down is a distinction between mandatory and voluntary *Control Points*.

Alternatively, new properties can be developed to cover design issues that were not present in the analysis. An example of a new property, and one that is currently under consideration, is that of *Information Salience*. This property focuses on the impact of certain metrics in other contexts. Religion for example is a very influential attribute and therefore has a high degree of salience. However, this *Information Salience* property might cause confusion and overlap with that of *Subject Coupling*. It is important to consider the relationship of the new property to the current properties, ensuring that there is no overlap or contradiction. Furthermore, new properties should be valid across different implementations of identity systems.

Another area for further development is the creation of a complete mapping between the individual properties and the potential outcomes that it can bring about. As an example, the analysis here has not identified how high levels of population comprehension might affect the lived experience, and therefore its impacts on the acceptance or rejection of an identity system. One could theorise, and seek proof of a situation where individuals might reject an identity system on the grounds that the population has a complete understanding of that system, thus enabling them to make more informed decisions on what may or may not acceptable. A complete mapping of the properties to potential outcomes would increase the effectiveness of the model in describing the lived experience. However, a degree of subjectivity is still needed. The mapping would only serve as potential indicators and would need to be judged in relation to the other properties, as well as the context of implementation.

Lastly, it would be beneficial to create an integrated framework that pulls in the various different approaches to create a complete human centred model. The aim of this proposed framework is not to replace the current approaches, but to supplement them aiding in a better understanding of how concepts of privacy and trust can be evaluated in terms of the system design. A comprehensive model that can be applied to various identity contexts would be highly beneficial to both practioners and researchers alike.

Conclusion

Identity is a pivotal construct in the interaction of an individual in a social space. Current approaches to designing human-centred solutions typically focus on the area of usability, privacy and trust. However, these approaches are utilitarian in nature seeking to create mechanisms that make it easier for organizations to collect an individual's information. They are abstracted from the reality of the situation in which the identity system is implemented. While these traditional approaches are important, we must be aware of their shortcomings, and acknowledge that the reach of identity beyond these realms.

It is an individual's identity that determines what he/she can or cannot do when interacting with others. Viewing identity as such extends the impact of identity beyond the point of interaction and data collection, shifting focus towards the practical impacts that identity has on an individual's life. Failure to acknowledge this effect of identity results in systems that can claim to be usable, privacy sensitive or trust worthy, but still result in systems that face rejection or systems that can have negative impacts for an individual. We need to take a step back from the identity system itself, and focus on the underlying relationships that are present in the identity eco-system. We need to consider the identity system in its context of operation, to analyse the system as a whole and determine its impacts on the lived experience. The framework proposed here aims to fill this gap, and act as a starting point for a genuinely human-centred approach to identity.

References

Adams A, Sasse M. Privacy in multimedia communications: protecting users. 2001. Available at: http://citeseer.ist.psu.edu/adams01privacy.html. Accessed 11 Feb 2008.

Aichholzer G, Strauß S. The Austrian case: multi-card concept and the relationship between citizen ID and social security cards. Identity in the Information Society. 2010:3. Available at: doi:10.1007/s12394-010-0048-9. Accessed 29 June 2010.

Ajzen I. From intentions to actions: a theory of planned behavior. In: Kuhl J, editor. Action control, from cognition to behavior. Berlin: Springer-Verlag; 1985.

Arora S. National e-ID card schemes: a european overview. Inf Secur Tech Rep. 2008;13(2):46–53.

Ashbourn J. Biometrics: advanced identity verification; the complete guide. London: Springer; 2000.

Backhouse J, Halperin R. A survey on EU citizen's trust in ID systems and authorities. Future of Identity in the Information Society; 2007.

BBC. All UK 'must be on DNA database'. *BBC*. 2007a. Available at: http://news.bbc.co.uk/1/hi/uk/6979138.stm. Accessed 28 June 2010.

BBC. Transcript—give us your DNA. *BBC*. 2007b. Available at: http://news.bbc.co.uk/1/hi/programmes/panorama/7040162.stm. Accessed 11 Dec 2008.

BBC, Ad system 'will protect privacy'. *BBC*. 2008a. Available at: http://news.bbc.co.uk/1/hi/technology/7280791.stm. Accessed 13 Aug 2010.

BBC. DNA database 'breach of rights'. *BBC*. 2008b. Available at: http://news.bbc.co.uk/2/hi/uk_news/7764069.stm. Accessed 9 Dec 2008.

BBC News. Facebook 'breaches Canadian law'. *BBC*. 2009. Available at: http://news.bbc.co.uk/1/hi/world/americas/8155367.stm. Accessed 13 Nov 2009.

Bennetto J. Police refuse to take DNA tests for database. The Independent. 2000.

Berthold O, Köhntopp M. Identity management based on P3P. In: Designing privacy enhancing technologies. 2001. p. 141–60. Available at: doi:10.1007/3-540-44702-4_9. Accessed 2 Aug 2010.

Bramhall P et al. User-centric identity management: new trends in standardization and regulation. IEEE Secur Privacy. 2007;5(4):84–7.

Burgoon J. Privacy and communication. In: Burgoon M, editor. Communication yearbook. Beverly Hills: Sage; 1982.

Camenisch J, et al. Privacy and identity management for everyone. In: Proceedings of the 2005 workshop on digital identity management. Fairfax, VA, USA: ACM; 2005. p. 20–7. Available at: http://portal.acm.org/citation.cfm?id=1102491. Accessed 2 Aug 2010.

Cameron K. The laws of identity. 2005. Available at: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

Caplan J, Torpey JC. Documenting individual identity. Princeton University Press; 2001.

Carroll WC. Fat king, lean beggar: representations of poverty in the age of Shakespeare. Ithaca: Cornell University Press; 1996.

Cavoukian A. Privacy by design: take the challenge. Canada: Information and Privacy Commission of Ontario; 2009.

Cavoukian A. Privacy by design: the 7 foundational priniciples. 2010.

Criminal Justice and Police Act 2001, Available at: http://www.legislation.gov.uk/ukpga/2001/16/contents. Accessed 20 Aug 2010.

Davies SG. Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. In: Technology and privacy: the new landscape. MIT Press; 1997. p. 143–65. Available at: http://portal.acm.org/citation.cfm?id=275289. Accessed 16 Apr 2008.

Davies S. The complete ID primer. Index Censorsh. 2005;34(3):38.

Decew JW. In pursuit of privacy: law, ethics and the rise of technology. Cornell University Press; 1997.

DNA database call prompts concern. *BBC*. 2007. Available at: http://news.bbc.co.uk/1/hi/uk/6979490.stm. Accessed 20 Aug 2010.

DNA pioneer Alec Jeffreys: drop innocent from database | Politics | The Guardian. 2009. Available at: http://www.guardian.co.uk/politics/2009/apr/15/jeffreys-dna-database-human-rights-police. Accessed 28 June 2010.

Fishbein M. Belief, attitude, intention, and behavior: an introduction to theory and research. Reading: Addison-Wesley Pub. Co.; 1975.

Fishbein M, Ajzen I. Belief, attitude, intention, and behavior: an introduction to theory and research. Reading: Addison-Wesley Pub. Co.; 1975.

Flick U. An introduction to qualitative research. Sage; 2002.

Garfinkel SL, et al. How to make secure email easier to use. In: Proceedings of the SIGCHI conference on human factors in computing systems. Portland, Oregon, USA: ACM; 2005a. p. 701–10. Available at: http://portal.acm.org/citation.cfm?id=1055069. Accessed 28 June 2010.

Garfinkel SL, et al. How to make secure email easier to use. In: Proceedings of the SIGCHI conference on human factors in computing systems. Portland, Oregon, USA: ACM; 2005b. p. 701–10. Available at: http://portal.acm.org/citation.cfm?id=1055069. Accessed 30 June 2010.

Giddens A. The consequences of modernity. 1st ed. Stanford University Press; 1991.

Goldacre B. Bad science: Home Office research so feeble someone ought to be locked up | Ben Goldacre | Comment is free | The Guardian. 2009. Available at: http://www.guardian.co.uk/commentisfree/2009/jul/18/bad-science-dna-database. Accessed 20 Aug 2010.

Goldberg I. Privacy-enhancing technologies for the internet, II: five years later. In: Proceedings of the 2nd international conference on privacy enhancing technologies. San Francisco, CA, USA: Springer-Verlag; 2003. p. 1–12. Available at: http://portal.acm.org/citation.cfm?id=1765300. Accessed 2 Aug 2010.

Graham E. DNA reviews: the national DNA database of the United Kingdom. Forensic Sci Med Pathol. 2007;3(4):285–8.

Graham EAM. DNA reviews: low level DNA profiling. Forensic Sci Med Pathol. 2008;4(2):129–31.

Greenleaf G, Nolan J. The deceptive history of the 'Australia Card'. Aust Qtly. 1986;58(4):407–425.

Guardian. Phorm: UK faces court for failing to enforce EU privacy laws. 2009. Available at: http://www.guardian.co.uk/business/2009/apr/14/phorm-privacy-data-protection-eu. Accessed 16 Nov 2009.

Hayles NK. Waking up to the surveillance society. Surveillance & Society. 2009;6(3):313–6.

Hoadley CM, et al. Privacy as information access and illusory control: The case of the facebook news feed privacy outcry. Electronic commerce research and applications. 2009, in press, accepted manuscript. Available at: http://www.sciencedirect.com/science/article/B6X4K-4W85MD0-1/2/b4c518bb554d998aa61320944e40ca94. Accessed 15 May 2009.

Hope C. Omagh bomb verdict sparks DNA review. *Telegraph.co.uk*. 2007. Available at: http://www.telegraph.co.uk/news/uknews/1573269/Omagh-bomb-verdict-sparks-DNA-review.html. Accessed 17 Aug 2010.

Hope C. Millions of profiles from DNA database passed to private firms. *Telegraph.co.uk*. 2008. Available at: http://www.telegraph.co.uk/news/uknews/law-and-order/2459976/Millions-of-profiles-from-DNA-database-passed-to-private-firms.html. Accessed 29 June 2010.

Inglesant P, Sasse MA. Usability is the best policy: public policy and the lived experience of transport systems in London. In: Proceedings of the 21st British CHI Group Annual Conference on HCI 2007: People and Computers XXI: HCI:.but not as we know it—volume 1. University of Lancaster, United Kingdom: British Computer Society; 2007. p. 35–44. Available at: http://portal.acm.org/citation.cfm?id=1531294.1531300. Accessed 28 June 2010.

Jain AK, Bolle R, Pankanti S. Biometrics: personal identification in networked society. Springer; 1999.

Jøsang A, Zomai MA, Suriadi S. Usability and privacy in identity management architectures. In: Proceedings of the fifth Australasian symposium on ACSW frontiers—volume 68. Ballarat, Australia: Australian Computer Society, Inc.; 2007. p. 143–52. Available at: http://portal.acm.org/citation.cfm?id=1274548. Accessed 2 Aug 2010.

Leitold H, Posch K. Austria citizen card: a bottom up view. In: Jerman-Blažič B, et al., editors. 2004. p. 247.

Leitold H, Hollosi A, Posch R. Security architecture of the Austrian citizen card concept. In: Proceedings of 18th Annual Computer Security Applications Conference. 2002. p. 391–400. Available at: 10.1109/CSAC.2002.1176311. Accessed 19 Aug 2010.

Ley BL, Jankowski N, Brewer PR. Investigating CSI: portrayals of DNA testing on a forensic crime show and their potential effects. Public Underst. Sci. 2010. Available at: http://pus.sagepub.com/cgi/framedrapidpdf/0963662510367571v1?. Accessed 29 June 2010.

Lips M, Taylor J, Organ J. Personal identification and identity management in new modes of E-government. Oxford Internet Institute; 2005.

Lyon D. Surveillance society: monitoring everyday life. Buckingham: Open University Press; 2002.

Lyon D. Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge; 2003.

Marks D, Yardley L. Research methods for clinical and health psychology. London: Thousand Oaks; 2004.

Martens T. Electronic identity management in Estonia between market and state governance. Identity in the Information Society. 2010;3. Available at: doi:10.1007/s12394-010-0044-0. Accessed 28 June 2010.

McCarthy J, Wright P. Technology as experience. Interactions. 2004;11(5):42–3.

Meints M, Hansen M. Study on ID documents. Future of Identity in the Information Society; 2006.

National Policing Improvement Agency. National DNA database annual report 2007–2009. 2010. Available at: http://www.npia.police.uk/en/14189.htm.

O'Donovan J, Smyth B. Trust in recommender systems. In: Proceedings of the 10th international conference on Intelligent user interfaces. San Diego, California, USA: ACM; 2005. p. 167–74. Available at: http://portal.acm.org/citation.cfm?id=1040830.1040870. Accessed 12 Aug 2010.

Omagh case review after verdict. *BBC*. 2007. Available at: http://news.bbc.co.uk/1/hi/northern_ireland/7149505.stm. Accessed 17 Aug 2010.

O'Neill S. DNA database under threat from European court, warns police chief. 2008. *The Times (UK)*. Available at: http://www.timesonline.co.uk/tol/news/uk/crime/article4083267.ece. Accessed 16 Aug 2010.

Orr J. Judge wants everyone in UK on DNA database | UK news | guardian.co.uk. 2007. Available at: http://www.guardian.co.uk/uk/2007/sep/05/humanrights.ukcrime. Accessed 28 June 2010.

Parliamentary Office of Science and Technology. The national DNA database. London: POST; 2006a.

Parliamentary Office of Science and Technology. The national DNA database. Parlimentary Office of Science and Technology. 2006b. Available at: http://www.parliament.uk/documents/upload/postpn258.pdf. Accessed 21 Nov 2008.

Pfitzmann A, Hansen M. Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management—a consolidated proposal for terminology. 2008. Available at: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.28.pdf. Accessed 24 Apr 2008.

Rayner G, Gammell, C, Britten N. Madeleine McCann DNA 'an accurate match'. *Telegraph.co.uk*. 2008. Available at: http://www.telegraph.co.uk/news/worldnews/1562710/Madeleine-McCann-DNA-an-accurate-match.html. Accessed 28 June 2010.

Robbery conviction overturned. *BBC*. 1999. Available at: http://news.bbc.co.uk/1/hi/uk/258367.stm. Accessed 16 Aug 2010.

Science and Public Protection. Keeping the right people on the DNA Database. United Kingdom: Home Office; 2009.

Silcock R. What is E-government? Parliam Aff. 2001;54(1):88–101.

Smith HJ, Milberg SJ, Burke SJ. Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly. 1996;20(2):167–96.

Sokolov D. Österreichs größtem Signatur-Anbieter droht die Pleite. *Heise Online*. 2006a. Available at: http://translate.google.com/translate?hl=en&ie=UTF-8&u=http%3A%2F%2Fwww.heise.de%2Fnewsticker%2Fmeldung%2F68944&sl=de&tl=en&history_state0=.

Sokolov D. Österreichs Signaturanbieter A-Trust sucht den Weg aus der Krise. *Heise Online*. 2006b. Available at: http://www.heise.de/newsticker/Oesterreichs-Signaturanbieter-A-Trust-sucht-den-Weg-aus-der-Krise–/meldung/69316. Accessed 9 Jan 2009.

The Independent. The McCanns: unbelievable truth or unimaginable nightmare? The Independent. 2007. Available at: http://www.independent.co.uk/news/world/europe/the-mccanns-unbelievable-truth-or-unimaginable-nightmare-402486.html.

The Register. Japan rolls out national ID registry. The Register. 2002. Available at: http://www.theregister.co.uk/2002/08/07/japan_rolls_out_national_id/. Accessed 3 Apr 2008.

Thompson WC, Taroni F, Aitken CG. How the probability of a false positive affects the value of DNA evidence. J Forensic Sci. 2003;48(1):47–54.

Torpey J. The invention of the passport: surveliiance, citizenship and the state. Cambridge: Cambridge University Press; 2000.

Turow J, et al. Americans reject tailored advertising and three activities that enable it. In: SSRN eLibrary. AusCert. 2005. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214#. Accessed 16 Nov 2009.

Whitehead T. DNA fingerprint pioneer brands database ruling 'very disturbing'. *Telegraph.co.uk*. 2009. Available at: http://www.telegraph.co.uk/news/uknews/5293393/DNA-fingerprint-pioneer-brands-database-ruling-very-disturbing.html. Accessed 16 Aug 2010.

Workgroup on User-Centric Identity Management. Empowering individuals to control their personal informaiton. Wilmslow, United Kingdom: Information Commissioner's Office; 2008. Available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/wgucidm_report.pdf.

Xin L. Trust in national identification systems: a trust model based on TRA/TPB. Washington State University; 2004. Available at: https://research.wsulibs.wsu.edu:8443/dspace/bitstream/2376/217/1/Xin_Li_071304.pdf. Accessed 31 Jan 2008.