IDIS (2008) 1:39–53
DOI 10.1007/s12394-009-0006-6

Towards a better citizen identification system

Piotr Cofta

Received: 19 September 2007 / Accepted: 7 July 2008 / Published online: 20 February 2009

Abstract Citizen identification systems (known also as 'ID card systems', or 'national identity management systems', even though those definitions are not identical) are receiving a mixed acceptance, with their privacy, security and usability being criticised, specifically in the UK. This paper investigates whether it is possible to improve social acceptance of such systems in cases where they are incompatible with the perceived value of privacy, but without significantly changing their original architecture. The paper analyses requirements using four different scenarios that address long-term privacy issues. Relatively small alterations to such systems are suggested that may significantly improve their adoption.

Keywords Identity management · Privacy · Technology acceptance · Trust

Introduction

Citizen identification systems (interchangeably yet incorrectly known also as 'ID card systems', or 'national identity management systems', as those terms are not identical) are having a rather bad press these days, specifically in the UK where the scheme has been enacted by the Identity Card Act (2006) and its deployment is being staged from November 2008 onwards (BBC 2008). There is a heated discussion about the viability or such system considering associated risks, danger to civic liberties and technical challenges. At the same time projects experience cost overruns, security blunders, sudden changes in specification, and overall unclear political agenda (London School of Economics 2005). The image of public disenchantment combined with entrenched interests looks as yet another expensive failure.

P. Cofta (✉)
BT Innovate, British Telecom, OP13, Polaris House, Adastral Park, Martlesham IP5 3RE, UK
e-mail: piotr.cofta@bt.com

This paper however neither criticises the premises of such systems nor uncovers their weaknesses. Instead, this paper explores the technical prerequisites for the social adoption of such systems, i.e. it attempts to capture such technical properties of the system that may make a difference to its acceptance while still satisfying the core purpose of the system.

The paper starts from observations on identity and identification, to investigate the position of citizen identification systems. From there, the investigation into a process of social adoption leads to the understanding that long-term privacy concerns are the core obstacle. Four scenarios identify and present technical requirements. Discussion and conclusions close the paper.

Identity and identification

Identity, similar to trust and privacy suffer from a varied and disperse set of definitions. The following brief discussion points to four main notions of identity, and consequently of identification and identifiers:

1. Subjective psychology. Identity is understood as the individual's 'true self', the self-identity that can be defined as a self-reflective memory of one's body and mind, that should be continuously reconciled to construct the narrative of life (Giddens 1991). The integrity of such self-identity is essential for the proper functioning of an individual. Consequently, identification is the process of self-perception of internal integrity. The main purpose of identifiers is to express one's true self and its integrity.
2. Social sciences stress the social construction of identity as an interactive process of determining one's identity within and against the society (Tajfel and Turner 1979). Here, an individual defines himself as a member of various (potentially disjoint) groups, who is taking on various social roles. Identification and identifiers are used to strengthen this process where one demonstrates adherence to group norms and one is recognised by the group.
3. The operational definition of identity (supported by philosophy and logic) derives identity from 'being identical' and requests only that certain properties of an individual remain stable (identical) over time and space. The value of this operational approach is that while it may not deliver a clear understanding of what the identity is, it clearly links it with the process of identification, which is understood here as the assertion of the stability of one's identity. For that purpose, some actions (e.g. providing PIN), tokens (e.g. cards) or personal characteristics (e.g. fingerprints) are used as identifiers, in the expectation that the stability of identifiers guarantees the stability of identity.
4. The pragmatic (or technical) approach again links identity with the process of identification, as it defines identity as a set of attributes that is sufficient to distinguish between entities within a given context and for a given purpose (Pfitzmann and Hansen 2008). This definition stresses the uniqueness of identity (within a context) but also introduces the notion of partial identity and the relativity of identity (so that one entity can have several identities, albeit in

different contexts). Names of different kind (give names, login names, pen names) are primary examples of such identities within the social domain.

Both pragmatic and operational definitions have been widely adopted by information security and from there they became a foundation of several information-based systems, including citizen identification ones. Unfortunately, conflicts between those four different definitions have not been properly addressed and are still a source of a significant weakness to our understanding of identity, giving rise to opportunities of identity theft.

Specifically, the process of identity verification (confusingly known also as authentication), designed to increase the assurance of the binding between different identities, becomes a source of weakness. The typical example is the acceptance of physical credentials or knowledge as surrogates for the guarantee of self-identity. As the operational identity of credentials is guaranteed only by the continuity of ownership and the identity of knowledge only by the continuity of non-disclosure, neither is immune to abuse. Similarly, a possible discrepancy between one's identity as a person and one's changed social roles (hence responsibilities, authorities and entitlements) can easily lead to abuse. Furthermore, even the identity of mind and body does not guarantee the identity (even less the benevolence) of intentions. Various procedures, such as revocation or profiling, external to the technical system itself, are deployed to minimise the impact of such weaknesses.

Citizen identification system

Technically, citizen identification systems are quite straightforward as they all follow the concept of trust management systems (Blaze et al. 2003) that they share with e.g. access cards or credit cards. While several architectures may exist, they usually follow the same pattern: a central database and 'identity cards' that are issued to citizens. Variations are related to the location and content of the database (or several distributed yet cross-linked databases), the content and technology of the card (size, security), communication architecture etc.

Similarly, processes supported by such system are not much different from credit or loyalty card schemes. During the enrolment process an individual receives the card that can be subsequently used at participating points to obtain access to goods or services. Such processes well support what is seen as the main purpose of the citizen identification system: to improve assurance of citizen's identity in their dealings with the state.

This relatively narrow definition of the purpose of such a system makes it particularly irrelevant to the rich experience individuals are having with their identities. The system does not cater for group identity (in fact, it does not cater for an identity of anyone else than the individual, be it business, government agency or charity organisation). Furthermore, it does not allow for the maintenance of several presentations, the subject that deserves separate discussion. It is also not directly concerned with entitlements, even though there is a strong tendency to link the database with a repository of deontic rules related to the citizen, in the form of

obligations (e.g. the citizen has to pay taxes) and entitlements (e.g. the citizen can use the heath care system).

Note here that both terms: 'citizen' and 'state' are used here at a relatively high level of abstraction. The term 'citizen' encompasses all the individuals that can participate in the system and—depending on particular solution—it may include not only rightful citizens, but also permanent residents, refugees, long term visitors etc. Similarly, the 'state' is not a monolithic institution, but rather a collection of agencies that may be driven by slightly different political goals, and that potentially employ a significant number of 'citizens' (so that they are also users of the identification system).

There are certain perceived social benefits of a citizen identification system, yet countries differ in realising them. Such a system is believed to significantly improve the efficiency of service delivery, decrease the overall cost, improve border control, simplify everyday experience in contacts with a variety of institutions etc. While its ability to contain terrorist attacks is questioned, the usefulness of a good citizen identification system should not be overlooked. Some countries have significantly benefited from the centralised identification of its citizens, while several countries have already introduced or are considering an introduction of such systems. However, within the EU, there is very limited trust in institutions that administer such scheme (Backhouse and Halperin 2007).

Significant risks associated with improper design or operation may quite often offset any perceived benefits. Such system poses a risk indeed, both directly (e.g. if personal information becomes compromised leading to large scale identity theft) and indirectly (where it can be used as a platform to cross-link surveillance systems and to restrict civil rights). Both risks are real and while their likelihood may be discussed, the size of a negative impact must not be overlooked. Specifically, privacy as well as other personal rights can be significantly violated either as a result of intentional information sharing or by direct attack on the system.

From the information security perspective, a personal identification system may be considered to be a rather risky proposition (Solove 2003). As the central database is the most vulnerable part of the system and assuming the operational lifespan of information within the system of 80 years (i.e. the life expectancy of the citizen), incentives to share and to attack are enormous to the extent that one can assume that the database will be compromised during this time, regardless of technical countermeasures taken.

Technology adoption

Research in technology adoption (acceptance) demonstrates two distinctive streams. The first one analyses the process of personal adoption, seeking clarification regarding decisions made by individuals, on the assumption that individuals are relatively free and well informed to accept or reject the given technology. The Technology Acceptance Model (TAM) (Davis 1989) is a well known example of the conceptualisation of this process, where ease of use is seen as a driver to usefulness, both influencing intentions to interact and finally use the technology. The richer

UTAUT model (Venkatesh et al. 2003) also addresses components that relate to social influence.

Another stream addresses the social adoption of technology, where an individual decision to adopt is embedded into the structure of social relationships. Some research addresses technology adoption and diffusion (Isham 2000) to investigate how individual decisions are affected by the socially-embedded dissemination of knowledge and practice. It is commonly observed that both diffusion and adoption follow social relationships, i.e. if individuals and groups that are trusted adopt the given technology; they are followed by those who trust in their choice.

A compatible, yet alternative view is provided by an analysis of the relationship between society and technology (rather than individual decisions), to analyse the value compatibility between technology and the society. It has been demonstrated that such compatibility with regards to value and structure greatly improves technology adoption.

For example, a multi-dimensional analysis of the value compatibility of the information system within the corporate environment (Bunker et al. 2006) shows that even if structural and practical dimensions of compatibility can be satisfied, adoption can be hampered by perceived cultural incompatibility. This demonstrates the difference between a formal recognition of trusted relationship (as embedded in organisational structures and practices) and informal ones (mostly reflected in the corporate culture). This case study also shows how employees respond to the perceived incompatibility by innovating practices around such incompatible technology, often contravening the original intent of the deployment.

Not considering regulated societies of corporations but self-regulated nations, Bohmann (1989) addresses the concept of social compatibility of technology, defining a desired set of values that should be embedded in the technology, in the form of a postulate proposition that should benefit the society.

Adoption of identification systems

The nature of citizen identification systems is that real benefits of such systems can be captured only when they are universally adopted. For as long as such an identification system is only one of several that must be dealt with, the system is more of a burden than of value, for the state, its citizens and potentially also for businesses. Therefore, assuming that participation in such system is voluntary; its success depends greatly on its adoption.

The adoption of technical systems is driven by the perception of risk assisted with its operation (Lacohee et al. 2006), much more than by the trust in its operation, as technology itself is no longer trusted. On the basis of available information, citizens estimate whether the technology proposition offers a fair deal—i.e. whether potential benefits outweighs potential costs and problems, including system failure.

If the adoption is desired, this observation opens up two possible paths that should be explored in parallel: one that increases perceived benefits of the system, and another that addresses its shortcomings. In the case of identification systems the first one may lead to coercion (so that citizens will be forced to comply, and non-

compliance will be punished) or to bribery (so that citizens will be offered certain benefits in exchange for adoption).

While the first adoption path may be beneficial for the initial adoption of the system, it will not guarantee the long-term acceptance that depends on addressing and minimising problems. Therefore this paper concentrates on this second adoption path where possible shortcomings of the system are addressed.

Of several potential concerns and perceived shortcomings, concerns related to citizen's privacy are the most important ones (Lacohee et al. 2006), (Information Commissioner's Office 2006). Such concerns arise from certain architectural and operational elements of the system: its state-wide pervasive nature, concentration of personal data, persistent records of various activities as well as the inability to withdraw from such a system.

Such privacy problems can be addressed easily if there is trust in the operation of the state, as the desire for privacy quite often signals a lack of trust and can be compensated by it (Cofta 2008). Some of the successfully operating systems rely on such trust. However, in the case of the UK there is very little trust in the state, as its motives, competences and integrity are questioned (Lacohee and Phippen 2007).

The notion of value compatibility offers a perspective that may be useful here. The identification system is not only a tool to achieve certain ends, but it is also a communication from the state regarding its intentions. Here, technical and operational components of the system are interpreted by citizens as signals of values that the state is willing to uphold. If they find those values compatible with theirs, the system may be willingly adopted, despite its other potential shortcomings.

Privacy-related value compatibility creates its own virtuous loop. As privacy seems to be a value that citizens are concerned with, the system has to demonstrate that it takes such concerns seriously to drive adoption. However, such privacy-related communication contributes to the perception of trustworthiness of the state, so that eventually it may alleviate the source of worries related to privacy: those of a lack of trust in the state.

This brings the question of what is the privacy that is being discussed here. Indeed, considering the number of partly conflicting definitions of privacy, such an operational definition is needed here. The concept of 'privacy as contextual integrity' (Nissenbaum 2004) defines privacy as compatibility with presiding norms of information appropriateness and distribution, i.e. the privacy is preserved if information flow of personal information adheres to norms and standards as perceived by an individual. Therefore, information disclosure, collection and processing that is expected and approved of by individuals do not impinge on their privacy. However, activities such as secret information sharing, use of information beyond its original purpose, information linking across domains etc. negatively impacts on the privacy.

In the light of value compatibility, this definition of privacy brings an additional insight, as it is the compatibility of norms and values regarding information flow that both defines and upholds privacy—provided that there is not a great discrepancy between norms and their implementation. Should citizens and their state be in accord with the norms regarding information processing, their privacy will not be endangered. The citizen identity system is therefore not only a technical solution

to certain problems, but it is first and foremost the message sent by the state describing norms and values that it wants to uphold.

Note that the specific role of the state warrants much deeper discussion regarding such values than is necessary for a similar commercial system. While there is no significant technical difference between an advanced loyalty or credit card scheme and a citizen identification system, their value proposition and the strength of the required commitment is quite different, as commercial systems tend to communicate value that is linked to brand promise.

For customers, such value compatibility is non-obligatory and non-binding: should they become unhappy with one brand (and one scheme); they can always switch to another one, which promises to reflect their values more closely. In contrast, there are no competing propositions from the state, and the commitment is effectively life-long (discounting the possibility of migration).

Scenarios

The most important single actor of an identification system is the state, and the adoption of the system depends mostly on values that the state demonstrates through the deployment of the system and its current and future operation. It has been already determined that one of the most important values that the state should address is the privacy of its citizens, therefore the analysis below concentrates on the role of the state in addressing privacy.

Casual observations may lead to the early conclusion that the state is not interested in the privacy of its citizens. Indeed, such privacy may be seen as being overly self-constraining, preventing efficient delivery of services, increasing the complexity of solutions, making innovations harder etc. However, it should also be understood that the state is neither monolithic nor static.

An analysis of the state's approach to privacy should look beyond what is available now and here, as the state forms a dynamic environment (legal, political, economical etc.) of several agencies in which the system will work for quite a long period of time. The state is driven by political will and can alter such will in the course of time (e.g. as the outcome of election, rearrangement of its priorities or as a response to external pressure). The desired identification system should be therefore able to operate in a variety of configurations.

Therefore, a scenario-based approach is taken. From the perspective of privacy impact on the identification system, and provided that the social perception of privacy does not change, the following four scenarios are considered, covering the majority of potential future development paths that the state can follow. Each scenario delivers a different set of features that will be later used to formulate specific requirements towards a better identification system.

Benevolent state

This is the most optimistic scenario that assumes that the state operates reasonably flawlessly and acts in the best interest of its citizens. While certain imperfections

may exist, the major political will of a state is that of serving citizens and not engaging in any activity that may decrease their perceived privacy.

Within the scope of this scenario, several worries traditionally associated with the identification system (such as the risk to privacy or civil liberties) are non-existent. However, this scenario requires a high level of public trust in the state itself. Such trust should be built on a sustained flow of evidence of trustworthiness, otherwise the public will realise at a certain moment that they have been coerced or tricked into trusting the state.

Assuming that the state is truly trustworthy, the desired feature of the identification system is to continuously *deliver evidence of trustworthiness* of the state, so that citizens do not lose their trust. While such evidence may come in several forms, it is essential that the state is unable to deceive citizens with regard to its intentions, i.e. that evidences must not be easily faked and the trust they have in the state is justified (Cofta 2007).

Pragmatic state

This scenario assumes that while the state is not openly acting against its citizens, its continuous struggle to maintain the identification system (that has a significant life span), gradually erodes the idealistic approach of the benevolent state and shifts it towards a more realistic one. Specifically, in order to cover mounting operational costs and to increase operational efficiency, the state may allow third parties (e.g. big business) to participate in the system.

There may be several forms of such participation, from the outright data mining of a large database to the use of the card for identification of customers, to more subtle private–public cooperations. For example, the state may outsource the actual operation of the system to private businesses, leaving for itself only a regulatory role. Such businesses therefore not only have access to large parts of the system, but can also repurpose it for its needs.

As business is not driven by political will but by commercial efficiency, this realistic approach may easily lead to a situation where the original purpose and principles of the system are lost in incremental extensions of its scope ('function creep'). As the ownership of the system becomes unclear, confusions regarding value compatibility will increase. Specifically, data leaks to commercial systems that are processed for profit may lead to the destruction of trust in the system and to the damage of its operational efficiency.

The most important feature of the system is therefore to *minimise function and information creep* that may appear as commercially-driven partners will gain access to data stored in the system. While each individual access may be hopefully justifiable in terms of efficiency, usability or legal enforcement, its cumulative effect on value compatibility must be monitored and averted.

Incompetent state

While the state may not be less fortunate when it comes to failed ICT projects, its problems are more visible. In fact, once significant security blunders (BBC 2007) are factored in, it may seem that the incompetent state may be quite dangerous. For

reference, in 2007 in the UK there were 36 million private records lost or misplaced by the state. Considering that there are more than 60 million people living in the UK, it is a significant majority of the population that has been already exposed to the risk of identity theft by their own state.

This scenario assumes that the state intends to operate the identification system, potentially in a pragmatic way, but due to its incompetence it allows data to be stolen, misplaced, altered or otherwise abused. The accessibility of data may attract criminals, but it may also attract causal snoopers, large businesses or agents of another (not necessarily friendly) state.

In this scenario, technical and procedural security provides a rather illusive reassurance specifically that the incompetence of the state implies that security will be incomplete and fragmented. Considering that humans are the weakest part of any security, and that a significant number of successful security attacks are done by insiders, it is only a question of time before data becomes compromised.

Therefore, from the perspective of a citizen, the question is not whether data will be lost or stolen, but what is the process once it is lost or stolen. Consequently, the requirement here is not about a perfectly secure system, but about a system that provides *detection and restitution* mechanisms, so that data breaches can be identified and citizens can be somehow compensated.

Malicious state

The fourth scenario assumes that the state has installed an identification system but that in time the operator of such a system has changed to be malicious. This may be the effect of a political coup, but it may be also the effect of a system being compromised by an organised crime—and considering the expected lifetime of a system, such a transition may be a likely event.

The new operator may use the system for purposes not originally intended, e.g. to introduce a totalitarian regime where unwanted individuals will be monitored, retained and eventually exterminated. Who and why will be subject to such coercion is highly unpredictable, as every conceivable differentiating feature (e.g. sex, religion, skin colour, health state etc.) can be used.

The feature that is essential here is the ability of the system to *contain the catastrophe* that may be introduced if a malicious state takes over control of the identification system. Negative impact of such a hostile takeover can be prevented only if a significant amount of operation is in the hands of individuals who may eventually opt out from the system. While such a feature may conflict with e.g. the need for efficiency, it is essential for the safety and the adoption of the system.

Requirements

From the analysis of the four scenarios above, it can be seen that there are five requirements that are essential to minimise the perception of risk of such system, thus potentially driving the adoption of it. While each requirement is primarily driven by one of the scenarios described above, they are visible throughout al or most of the scenarios.

Deliver evidence of trust

Convincing citizens to trust the state with regard to the identification system may be actually less hard than expected. The old adage 'nothing to fear–nothing to hide' has been applied for a long time to citizens, but it works equally well when applied to the operation of the state. If the state is trustworthy, then the only question is how to deliver evidence of it.

While an average individual may never fully comprehend the intricate details of the identification system, he is at the same time the best guardian of the integrity of the system. He is both vitally interested in protecting his own identity and he is a keen observer of the way such identity is used (and abused) by various institutions. In fact, the state can possibly convert most of the opponents of the system into voluntary participants (as controllers and verifiers) if the system provides tools for them to act as such.

What is needed is a *high level of operational transparency* at least at the level provided by leading e-commerce web sites today (so that it is not beyond technical means to deliver it and is not beyond human means to benefit from it). Ideally, every access to every record that is relevant to an individual should be recorded and could be viewed by such an individual—possibly on-line, using the card that is already in his possession.

Not only this: in a fashion similar to the feedback that is both desired and dreaded by e-retailers, every improper operation can be *publicly contested and verified*. Should an individual believe that his information has been mishandled, he may seek a legal recourse (that is usually inefficient), or he may resort to a less expensive yet strikingly efficient way of attaching his feedback to the record of such an operation. Statistical algorithms can be deployed by independent bodies to see whether records have not been tampered with (e.g. by a state official that is too eager to hide improper operations) and whether the system as a whole operates in a reliable manner.

User-centric identity management may provide yet another set of tools to instil trust, this time by allowing citizens to be guardians of their personal information, i.e. by removing the need for potentially excessive amount of initial trust. Such a system may allow citizens to learn to trust the state (assuming that the state can demonstrate its trustworthiness), offering the development part that leads from extensive control to mutual understanding and eventually to trust (Lewicki and Bunker 1995).

The technology described here is available and is already in use today. While the scale, complexity and exact details may differ from what is correctly used, there is nothing that inhibits this approach. Transparency and shared control is always seen as a significant sign of trustworthiness and it also provides strong prevention measures against excessive information creep.

Offer fair deal

Function creep may seem to be unavoidable in the longer term, but the main concern of individuals is not that it may happen, but that they are not part of it, i.e. that they are bound to bear an additional burden and cost while not receiving anything. The modern, educated customer is aware that the state financially benefits from function

creep, either by decreasing its operational cost or by receiving profits from providing identity-related services to businesses.

While individuals expect to receive certain benefits, the fulfilment of such benefits lies mostly outside of the technology part of the system. However, the technology should provide individuals with tools that allow them to monitor such deals and to verify the fairness of the deal. Such goals may be achieved e.g. by *consensual data sharing* where individuals will be explicitly asked whether they would like to participate in a particular deal.

Should the consensual data sharing become problematic (e.g. due to the amount of data or the complexity of business deals), an alternative is to allow citizens to monitor data sharing agreements, so that they are neither surprised nor unprepared for new applications of the identification system.

Provide detection and restitution

While the perception of the fallibility of technology is quite pervasive, this does not prevent individual from adopting such technology, as long as certain restitution measures are provided to restore the state before the failure or at least to compensate for the losses. Such restitution measures are usually embedded outside of the technical system, but they impose certain requirements on the technology used.

The centrally issued identifier (such as card) is potentially an attractive proposition for both businesses and individuals to assert identities, but such an assertion may not be backed by the state in the form of any assurance or assumed liability. Furthermore, the state is unlikely to assume any significant liability for eventual losses accrued by individuals in case data from the central database is compromised.

While this may be seen as unfair (specifically comparing with requirements that the same state imposes on businesses and individuals), such decisions are not necessarily detrimental to the ability to provide restitution, for as long as the system enables others (presumably private businesses) to provide such restitution, e.g. in a form of identity insurance. As a minimum requirement, such businesses, as well as individuals should have *access to information that is stored in the system*, should have the ability to review and effectively contest such information (including any audit or log files that the system produces).

Examples from the financial industry demonstrate that such restitution measures are neither impossible nor excessive, but that they instil the perception of shared ownership and responsibility of data, with individuals voluntarily assuming the uneasy role of data controllers and verifiers.

Guarantee safety

The potential catastrophe of the malicious state calls for system safety, i.e. the system's inability to harm individuals. This leads to a requirement to balance the power between centrally a controlled database and individually held cards, a requirement that also contains function creep. While cards are issued by the state and the database is operated by the state, the design can *make the database useless without a card*, thus reducing the scope of a possible disaster and decrease incentives

to repurpose the database. This requirement intentionally restricts the functionality of the central database, thus removing a certain power from the state and placing it in the hands of individuals, further contributing to the perception of trustworthiness.

Technically, this calls for a re-design of authentication, provisioning and revocation, where the ownership of data ultimately is granted to an individual. Authentication itself does not need excessive information about an individual to be stored unprotected in the database, as it is concerned mostly with the validity of the card. Provisioning requires identification, but once the card is issued, this data can be tied to the card (even if stored centrally), e.g. through encryption. Finally, agreed revocation procedure should allow an individual to remove compromised records and to the re-issue the card.

If the requirement to render the database record useless without a card may be impossible to achieve, certain protection can be achieved by distributing the database. This again brings the notion of multiple identities (discussed later) that can be used here not only to satisfy human needs, but also to improve the balance of power, and to decrease the risk of catastrophic failure as well as to improve the operation of the scheme. The use of *federated authentication* systems allows information distribution (hence risk) across several schemes, including commercial ones, leaving the government with the task of standardising, overseeing and inter-linking such schemes.

None of technologies described here is complex and none is novel. In fact, systems that adopted some of these requirements have been in operation since late 1960s. The technology choice may seem to be unnecessarily self-restraining (specifically if the state thinks of itself as being a benevolent one), but this is a small price to pay for the ability to contain the catastrophe and minimise information creep.

Engage in a dialogue

Finally, as the society is always creative with new technologies, the identification system should not be deployed on a 'fire and forget' basis, but the state should *engage in a dialogue* with its citizens. It should be understood that the original deployment is only the first step in a continuous interaction between new technology and the society. Such creative interaction will require the state to monitor various new usage scenarios that will develop within the society together with social customs, norms and roles that are created as a result of the deployment of the identification system.

Such new norms and customs should not be seen as contradicting the main purpose of the system and should not be necessarily seen as a 'failure' of the adoption that should be 'repaired'. They should be rather perceived as the natural way for things to evolve, specifically for a system that does not fully conform to social norms. Such creative adoptions may imply certain alterations to the system (whether technical or related to its policies), but they do not necessarily undermine the main proposition of the system. The technical underpinning for such dialogue is the ability to *update the identification system* depending on needs.

The requirement for a continuous dialogue is not particularly demanding, given that other requirements lead to a system that already has several monitoring and

interaction tools. Apart from assuring that there are resources set aside for continuous research into implications of the identification system, the ability to deploy subsequent versions of the system is already common practice in the ICT industry.

Multiple identities and identifiers

It is widely recognised in the literature that both psychological and sociological understanding of identity stipulates that one person wants, may and can hold several separate identities (forming what can be called multiple personas or presentations of oneself) of one's true self that can be used in different social contexts (Turkle 1997). This may help an individual to manage the conflict between the desire for the integrity of one's self-identity and the necessity of modern social life to engage in several, sometimes conflicting, activities and groups.

More recently, multiple identities have been developed into a conscious strategy for privacy protection (Lacohee et al. 2006), where an individual maintains, generates and abandons significant amounts of short-lived identities, in an attempt to prevent excessive cross-linking between them.

The notion of separate presentation-identities can be seen as a contradiction to the intended purpose of a citizen identification system, i.e. to the ability to provide one assured identifier for each citizen. This is one of the reasons why the requirement for multiple identities did not emerge from the analysis presented here. However, closer analysis shows that they are both not necessary contradictory, and that the human desire to separate certain aspects of one's identity can be at least partly satisfied within the system.

First, the state itself is not a monolithic organisation and for the purpose of security and efficiency of its internal processes, it may want to restrict access by its own agents to personal information about the citizen. Certain states (Leitold 2006) have recognised those needs and deployed technology that effectively partitions the relationship between the citizen and the state.

Further, for businesses the separation of business-related identifiers from the state-issued ones (beyond the enrolment process) may be actually beneficial, as it contains business liability, fine-tunes the level of cost of security as well as allows for creativity and competition.

Note however that the separation that is discussed here is usually not technically perfect, as identifiers may be potentially cross-linked between the different domains and databases, should the state desire so. While ability to cross-link may be interesting for law enforcement, the illusion of separation may not be satisfactory for all citizens. This brings back trust in the state as essential to the process of adoption.

Conclusions

In the UK, there is a significant controversy surrounding the deployment of a state-wide citizen identification system. It is believed that several woes can be alleviated by properly analysing the required features and by demonstrating that relevant

requirements have been satisfied. Specifically, privacy seems to be of major concern to citizens who see the system as a threat to their liberties.

This paper offers an analysis of features and requirements for a personal identification system with the classical architecture of a central database and identity cards. By exploring value compatibility with regard to privacy through four scenarios related to the state, it has been possible to collect desired features of the system. Those features have been subsequently converted into five core requirements that can be implemented in technology and supported by appropriate policies.

It is believed that it is possible to shift the discussion from dire opposition to any identification scheme to one that analyses whether there are the properties of an acceptable (or even desired) system. If this is possible, then certain technical solutions can be used to ensure that particular requirements are met and that the system can be reasonably accepted. An example of such a system can be easily furnished to facilitate further discussion, whether in the form of a conceptual model or as a working demo.

The analysis presented here (including also at least some of the conclusions) can be applied not only to identification systems, but to other systems where the perception of a lack of privacy may hamper their adoption. Systems such as the NHS Connecting for Health (2005) where the consolidation of a large amount of personal information is combined with retention of such information over the lifespan of an individual may benefit from observations included here.

Acknowledgements The author would like to thank anonymous reviewers for their comments that greatly improved this paper.

References

Backhouse J, Halperin R. A Survey on EU Citizen's Trust in ID systems and authorities. FIDIS Journal (1/2007). 2007. http://journal.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf.

BBC. UK's families put on fraud alert (20 November 2007). 2007. http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm.

BBC. Q&A: identity card plans (06 March 2008). 2008. http://news.bbc.co.uk/1/hi/uk_politics/3127696.stm.

Blaze M, Ioannidis J, Keromytis AD. Experience with the keynote trust management system: applications and future directions. Proc. of First Int. Conf. on Trust Management iTrust 2003. Springer-Verlag LNCS 2003;2692:284–300.

Bohmann K. About the sense of social compatibility. AI and Society. 1989;3(4):323–31.

Bunker D, Kautz K, Nguyen ALT. The role of value compatibility in information technology adoption. In: Donnellan B, Larsen TJ, Levine L, DeGross JI, editors. The transfer and diffusion of information technology for organizational resilience. Boston: Springer vol. 206; 2006. p. 53–70.

Cofta P. Trust, complexity and control: confidence in a convergent world. New York: Wiley; 2007.

Cofta P. Confidence-compensating privacy protection. 2008. Submitted for PST2008: 6th Annual Conference on Privacy, Security and Trust, 1–3 October 2008.

Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly. 1989;13(3):319–40.

Giddens A. Modernity and self-identity: self and society in the late modern age. Cambridge: Polity; 1991.

Identity Cards Act. 2006. http://www.opsi.gov.uk/acts/acts2006/20060015.htm.

Information Commissioner's Office. 2006. What price privacy? http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf. Accessed 12 December 2007.

Isham J. The effect of social capital on technology adoption: evidence from rural Tanzania. opportunities in Africa: micro-evidence on firms and households. 2000. http://www.csae.ox.ac.uk/conferences/2000-OiA/pdfpapers/isham.PDF. Accessed 18 October 2007.

Lacohee H, Crane S, Phippen A. Trustguide: final report. 2006. http://www.trustguide.org. Accessed 5 January 2007.

Lacohee H, Phippen A. Trust and government in the UK—a grassroot perspective. 2007. Paper presented at the Trust Conference, The Hague, Netherlands, 21–22 November 2007.

Leitold H. Austrian citizen card. 2006. Presented at the eIDMeeting, London, 21 June 2006.

Lewicki RJ, Bunker BB. Trust in relationships: a model of development and decline. In: Bunker BB, Rubin JZ, editors. Conflict, cooperation and justice: essays inspired by works of Morton Deutsch. San Francisco: Jossey-Bass; 1995. p. 133–73.

London School of Economics. The identity project. An assessment of the UK Identity Cards Bill & its implications. Interim Report. 2005. http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDreport.pdf. Accessed 14 July 2006.

NHS Connecting for Health. Business plan 2005–2006. 2005. http://www.connectingforhealth.nhs.uk/resources/busplans. Accessed 12 May 2007.

Nissenbaum H. Privacy as contextual integrity. Washington Law Review. 2004;17:101–39. http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf. Accessed 10 June 2006.

Pfitzman A, Hansen M. Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management—a consolidated proposal for terminology (version v0.31 Feb. 15, 2008). 2008. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf. Accessed 20 June 2008.

Solove DJ. Identity theft, privacy, and the architecture of vulnerability. Hastings Law J. 2003;54:1227–73.

Tajfel H, Turner JC. An integrative theory of intergroup conflict. In: Austin WG, Worchel S, editors. The social psychology of intergroup relations. Monterey, CA: Brooks-Cole; 1979. p. 94–109.

Turkle S. Life on the screen: identity in the age of the internet. New York: Simon & Schuster; 1997.

Venkatesh V, Morris MG, Davis GB, Davis FD. User acceptance of information technology: toward a unified view. MIS Quarterly. 2003;27(3):425–78.