

Owning identity: one or many: do we have a choice?

Marcus Wigan

Oxford Systematics, Australia

Abstract

Identity is the key to linking records and multiple identities are the key to maintaining social functioning with appropriate anonymity, while retaining accountability. This paper addresses these factors and adds the issue of ownership of ones own 'identity'. Collapsing what are currently entirely legal multiple identities into a single identity through direct or indirect digital means has implications for dataveillance and surveillance. The lack of transparency in most such emergent developments amplifies an increasing asymmetry in information between government and major organisations - and citizens, the subject of this effect.

Keywords: identity ownership surveillance

1 Introduction

The rapid growth of databases, biometrics and RFID and other identity related technologies are approaching a critical mass as a potential means of controlling the population.

The **critical** aspects of these diverse technical advances are the links between identity and existing and **accelerating** intensification of dataveillance capacities. Taking one example: DNA databases are perhaps the most salient, but their comprehensive application is still to materialise in terms of a critical contribution on a large scale. The legal infrastructure to expand them more rapidly is already within the capacities enabled by recent legislation, but the cost and complication (and indeed vulnerabilities) in building such databases mean that at present we can consider them as simply fresh opportunities for function creep.

Salience, DNA might have, but its high profile potential is dwarfed by the already present risks inherent in the many other cross-linkages now being enabled **directly**. These links may be **direct** (via formal data matching legislation) or indirect by rapidly expanded powers ranging from authority to secretly monitor parties on a prospective (trawling) basis creating assemblies of data from many sources..

The linkages enabled by a “unique identity” are central to both direct and indirect means of data and physical surveillance.

Identity is now commonly publicly discussed and treated in legislation as if it were a unique item., . This supposition has many ramifications and impacts. One might surmise that these were emergent – or intended: in either case the social impact. is not widely appreciated.

2 What is Identity?

This is a basic question, and is assumed to be obvious. The classic *Compact Oxford English Dictionary*(referred to subsequently as the OED) (1984, p. 1368) definition is, after discussing sameness, likeness and oneness:

1. The quality or condition of being the same in substance, composition, nature, properties, or in particular qualities under consideration: absolute or essential sameness; oneness
2. The sameness of a person or thing at all times or in all circumstances; the condition or fact that a person or thing is itself and not something else; individuality, personality.

This definition demonstrates the ambiguity of the word. A clear distinction is drawn in the dictionary between the various definitions and usages of the term ‘identity’ and the quite separate term ‘absolute identity’.

Once again we profit from examining the full version of this definitive work on language – and find that the confusions and asymmetric interpretations used for the word are just as varied as the views on what identity comprises.

The penetrating point made by the OED authors is the choice of the phrase ‘in all circumstances.’” This is the critical factor that makes the verification of identity in one context assumed to apply to all contexts.

This is now the central issue.

There are few situations where complete and definitive verification of identity is possible, and the tendentious term “Identity Card”; simply makes the implied assumption that the token (the card) is indeed the person.

This is actually a big step, and one that has in the past considerably harder to do ‘in all circumstances’ than it seems.

“Identification” as a verb is the task that such tokens are aimed at addressing. Again, identification for what? It is hard to find a case where the context does not define the level of accuracy and reliability of the process of ‘identification’. Passports are specifically intended and agreed upon as the relevant token for border crossing (and in fact nothing else).

Yet the idea of a passport as a high grade token for assertion or verification of identity is almost irresistible as a simple means of establishing the identity of a person in situations far removed from any border. The intrinsic value of a passport as an identity token is explicitly exploited by hotels everywhere as a means of securing payment from the client – and to satisfy police and surveillance records.

Function creep will always be with us.

The most common form of identity is one’s name, but as there may be many with the same name the addition of a photograph provides additional discrimination. Yet an original birth certificate showing only the name is also deemed to be a high quality form of identity verification. ...

There are clearly far more factors involved in a “simple verification of identity” than meets the eye – and the OED has long been onto it.

In this paper **we** address the **different** factors that comprise identity in two ways:

1. The ability to achieve an accepted ‘identity’ as oneself by the use of tokens or other forms of associated factors
2. The level to which a restriction to a single token-certified ‘identity’ can or should be used for all purposes.

Once these rather different common interpretations of ‘identity’ are appreciated, there then becomes a clear need for multiple ‘identities’ sufficient for any specific purpose (usually a transaction, access or an event) requiring an assumed reliable association between a person and a token.

Many situations require only a temporary identity: a movie ticket is a simple anonymous example usually with a linkage period requiring a simple identity association of a very short duration (ie the holder is identified as authorized to enter the cinema: a very clearly defined context)– and with no attributes to be linked to a specific person required: the holder gets entry, non holders do not. Transaction completed.

Others require stronger links to the person and for longer. But it is clear that not only is there a working acceptance of an ‘adequate’ verification of identity, but there is also a recognition that not all events or transactions require the same identity to be used.

A professional woman may continuously operate in her unmarried name, a stage name, a *nom-de-plume* – or her husband’s surname in different circumstances. There is no suggestion made that this is in any way a criminal or even dishonest behaviour. On the contrary, many authors, actors, police, psychologists, witnesses etc all have valid and compelling reasons to be able to live under different identities. In the case of family violence or witness protection the lack of any linkages is imperative, sometimes for sheer survival.

How is it possible to have multiple identities in this way?

Simply because if people undertake their legal responsibilities with various bodies and the community this is a basic freedom – but this freedom depends on trust and genuine security and credible security at that.

The Tax Office has long had taxpayers paying tax on activities illegal at the time (prostitution being one example), and generated a solid reputation for keeping the ‘tax payer’ identity separate and unlinked to other forms of identity.

The current environment has dismantled these protections against linkage between legal multiple identities both by data matching and by huge reductions in the constraints on a range of public officers in many areas of state activity to access and link multiple identities.

This not only reduces the trust in these bodies, but also makes many people vulnerable in new ways. Family violence victims and witness protection programs are now not the only ones at risk. The pressures to eradicate multiple identities are associated mainly with efforts to link different forms of real time and recorded data and associate it with each individual for efficiency in establishing identity – and over time to build a cumulative and increasingly cross-linked picture of the person or thing ('entity') concerned. Tracing of behaviour, movements and characteristics and location of animals serves a similar purpose in scientific studies. Treating people as animals to be traced continuously wherever they go and whatever they do is an interesting perspective which is a disturbing facet of uberveillance, and emphasizes the potentially dehumanizing aspects of asymmetric information secured and held by anonymous third parties.

3 The Basis of Identity Verification

The efforts to make a token identical to a person are now mediated by computers and communications, where a single tag or number enables a person to be the subject to both intentional and generally undirected data trawling and integration.

The results of such trawls come up with links between people and activities – but are vulnerable to data quality, and other processes which may have been done for quite different purposes.

The issue of an initial verification of identity (say for a national ID card) is one of data quality – and this is an expensive commodity. The processes outlined for both the UK and the Australian national identity cards under consideration have huge holes in them.

These include the limited basis for verification before a person is approved as having demonstrated their own identity – and the very limited time allowed in most planning for such systems for this task to be executed. In the Australian system it is proposed that a brief training of Post Office works will suffice to execute this in a few minutes. For some a completely documented life record is easily supplied, but for others even securing people who have known them by sight and joint activities will be a real problem. Yet once the ID is issued it is assumed to be the unique identifier linked to the person in some real way. This will inevitably corrupt the ID database from the very start.

This means that false positives will be widespread not only for the person involved but other parties who have met 'higher' standards of verification. ...

This is an easily accepted argument – but is very misleading. Personal knowledge of a person covers many different attributes than simple appearance – yet a passport or driver licence with a photo ID on it is regarded as 'more reliable'. This is in spite of a large volume of evidence that people are very poor at matching photos to the relevant individual... as indeed are biometric facial recognition techniques at this point.

So how do we assess these issues?

As the major reason for government pressures for ID uniqueness, matching tokens is essentially to facilitate management and control of the population by longitudinal and cross-sectional linkages.

The rhetoric is to confirm right to access some location or service, or to be able to undertake a transaction - but this introduces a fundamental asymmetry in the relationship: false negatives in token matching deny access to those with the rights to them, with absolutely no penalty to government at all – while false positives allow such access and also contaminate the records of others thereby in both cases disadvantaging the population as a whole.

This basic issue of a single 'do all' Identity is simply not understood by many. This is not uncommon in cases of non-transparent information asymmetries between governments and the population as a whole. It is however an area where governance and identity interact.

A complementary view on some of these issues is given by Clarke (<http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html1994>)- but the over riding social aspect of such mappings onto a single unique (and indeed easily copied) digital identity is that of the inevitable denials of service, and most likely to those most in need of them as these are the people who will tend to have most difficulty in establishing their own identity in the first place.

4 Other Mechanisms

In non- governmental interactions trust is a major feature of transactions, and a recommendation, an introduction or even a simple referral can be quite sufficient for most transactions.

However, trust does not figure highly in everyday transactions with governments or large organisations. This links governance to transparency in the mediation of such interchanges requiring identity. Efficiency and cost savings are major drivers in the long- standing bureaucratic thrust towards universal unique identification.

The role of trust in government surveillance in the United States was discussed by Staples (1997) four years *before* the cultural shifts following the destruction of the World Trade Centre He argues that:

"The movement to a post modernist culture of corrections is one of normalising social control over all aspects of life - fit the power inequity aspects of privacy measured by others (p128)

"A society in a culture of surveillance, a society of judges exercising the power to punish everywhere, a society increasingly lacking in personal privacy and individual trust and a viable public life that supports and maintains democratic values and principles" (p129).

Were it not for function creep and the opportunistic approach of enforcement and other dataveillance and surveillance bodies, there might have been a high integrity medical ID card in Australia by now: yet this is one of the declared objectives of the Australian governments ID card initiative. Which has been described as carrying out many further functions from the start: demonstrated function creep before the system is even properly designed

The trust factor is still largely there between the community and the medical professions . Medical administration roles in handling and linking such data is not usually seen as part of the patient-doctor relationship. There are also asymmetries of information holding between doctors themselves is a consequence of the ownership of patient records by the doctor that treats the patient. These may be seen as barriers to efficiency, or as good faith in very private information held in trust – or, as is now increasingly the case in other fields, valuable commercial micromarketing data...

In summary, identification is clearly contextual, and efforts to move towards a unique token as formal ID can be seen to automatically trigger issues of governance, transparency and trust.

This perspective appears to replicate many of the aspects of the original Australia Card, the current Australian and UK ID card debates, but moves it on from the purely political aspects of power assertion to the mechanisms we have discussed.

5 Implementing Identity

So far we have avoided discussing the meaning of the tokens that are used as proxies or in support of identity establishment or verification. This now needs closer examination, as

there may be many tokens associated with a single identity – even when the individual is using one of several multiple identities.

A digital identity is an assemblage of token ('identifiers') that describe that identity. One person may have many personas (or operating or perceived identities), but for any particular function or transaction requiring the establishment of an identity for a specific purpose or occasion, there are usually only a few identifiers used,... and these may not be the same for transactions with another body or organisation.

In the contemporary, complex and high-paced world, organisations seek to manage identities on the basis of their digital identities. The quality of the management will reflect the quality of the digital identity. But that will vary enormously depending on the usual data quality characteristics (accuracy, precision, completeness, timelines, etc.), and especially on the quality of the acts of associating data with identities.

This leads us to the concept of a digital identity, which comprises solely a set of data associated with a specific person or thing. This set of data is assumed to be an accurate representation of the person or thing (the generic term for this is 'entity', and is a physical item or person).

There is a special set of digital data that is associated directly with an entity. Examples are

- in the case of a person, biometrics,;
- in the case of a person or thing and embedded RFID chips etc. In such cases the entity is its own identifier, and this is invariant on circumstances or situations requiring identity establishment or verification.

Organisations are seeking to manage entities on the basis of their digital entities. The quality of the management will reflect the quality of the digital entity. But that will vary enormously depending on the usual data quality characteristics \ and especially on the quality of the facts of associating data with entities.

If biometrics prove to be practicable in enough settings, the quality of digital entity may be higher than could ever be the case with digital identity.

The impact and implications are far more drastic, however, because the level of social control that can be achieved will chill individual behaviour, social discourse, economic innovation, and political thought and speech.

This qualitative difference between intrinsic (entity bound) identifiers, which stay the same for all circumstances, leads to an automatic deletion of multiple digital identities, as such a unique key to a person is virtually irresistible to both commerce (know your customer and tailor services to there their known wealth or other accumulated identifiers integrated over time), and to government for cumulative comprehensive population tracking and surveillance).

6 Links Between Surveillance and Identity

There is little difference in principle between:

1. An anklet with a GPS tag that is fitted to a prisoner to constrain his or her location, and to allow real- time monitoring as well as historical tracking of all his or her activities., and ;
2. An RFID location and access control badge that must be work worn to work to access or move about a specific building or area,;
3. An injected RFID chip to allow repeat Club patrons to be allowed to enter the premises- and of course potentially to be monitored by other detectors.

The real difference is the voluntary nature of some of these identifiers (injection of an

RFID chip) and the nature of the usages made of the data stream that follows: voluntary or not (intrinsic identifiers such as biometrics or DNA are not voluntary).

Context is all. As long as the context is the domain solely of –say - a Club premises, then multiple identities are still possible outside that domain – but if this unique tag (or biometric) is accessed by other organisations, then (in the case of biometrics) an indelible trail is cumulatively created-: one that can be readily extended backwards and well as forwards, and over many organisation both prospectively or historically.

This process is the collection of a surveillance data set. The links between surveillance and identity depend critically on the tokens or identifiers used to establish identity. Persistent identifiers specific to the person or thing (entity) make it very difficult to avoid function creep.

The scope of intrinsic identifiers is global, the differences are in the ease or otherwise of securing them. As costs drop in securing and converting intrinsic identifiers then the application widens rapidly. DNA databases used to be collected solely from criminals, but are now routinely collected from suspects who may be innocent. Function creep has already occurred with the general public in the area of an event now having their DNA required as prospective scanning and profiling tool with the data being retained to build on ever expanding databases..

In whatever way it proceeds and under whatever guise, such libraries of intrinsic identifiers can only grow and expand.

National ID cards are specifically designed to make this possible. There is no need for automatic ticketing cards to include high grade identification, but the emergent practice is that it will be. The anonymous token (paper ticket) simply does not provide enough marketing and trace information for the various parties – commercial and enforcement— seeking it as a by- product of your purchase and use of a right to travel from A to B. The days of anonymous travel or movement are numbered.

As such cumulative records emerge, then the existence and use (let alone the well documented tendency for abuse) of surveillance data will affect the social space of all the surveillance subjects (ordinary citizens)., Such constraints on social space have a disproportionate effect on individuals who need to live with multiple identities (or to have to alter) their identities.

The only way to conserve the existing legal right to operate using multiple identities is to require a privacy audit of all systems and digital tokens used. This is quite evidently not in the interest of many parties seeking such surveillance and retrace capacities, and, as a result is highly unlikely to occur. Abuse (as is so well documented already (e.g Independent Commission against Corruption,1992) will occur- and both the social space with be reduced and the security of individuals concerned will become at greater risk as a result.

The shrinking of social and physical space has already been observed. As a result of the intrusive and extensive biometric data capture and distribution at the borders, there are numbers of people who have simply stopped traveling on routes that require entry to the USA.

7 Collapsing Identities

The surveillance aspects of digital identity tracking also lead to a substantial contraction of the social and transactional spaces that people can use. Examples are already plentiful. CentreLink requirements for identity documents from the very groups most likely to not ever have had them, simply are a plausible and defensible means of denial of access.

Currently the tests required to establish identity include known persons and other normal social means of adequate identification for the purpose in hand... but once unique (or quasi-unique) digital identity tokens are held by all, then there will be two major effects:

1. Such low grade data entering the system as many simply will not have the levels of documentary 'evidence' of their identity (leading to both positives and false negatives in the use of the supposedly unique digital identity), and a general reduction of the integrity of the whole system
2. Lack of the token will enable denial of service.

It is clearly necessary to introduce a concept of Contextual Sufficiency into identity establishment. This has been in the past implied in almost all transactions, but will be lost if all one's identities are required to be collapsed into one via the existence of a unique identifier;.. and if this is a biometric, the contextual variations and relaxations will be lost.

Once the principle of Contextual Sufficiency is lost, then validation failures and multiple matches will have pervasive and widespread negative effects on individuals- and this will not be restricted to those with a major need for multiple identities right now.

The marked increase in information asymmetries between the observed and the observers will require compensating social action. One essential action must be the removal of politicians exemption from privacy laws applied to their data collections. Other less obvious steps will be needed as well to provide transparency and accountability for linked or potentially linkable information resources. Brin (1998) discusses an interesting highly speculative but stimulating case of full symmetry of information between the surveillers and the surveilled. If only such a scenarios could be realistically envisioned, let alone implemented, but it goes against the pervasive enforcement organizations and political structures in most present cultures and societies.

It is clear from public debate that the pervasive impact of collapsing identities to one for each person introduces many restrictive and disturbing side effects and vulnerabilities. These will grow with time, rather than diminish, due to the retrospective matches that will become possible.

8 Ownership of Identity

As almost all tokens of identity are now handled in a digital form, operational identity is becoming a bundle of data items. Who owns these?

The current TRIPS¹ protocols of the World Trade Organisation (WTO) is very clear on this:

1. Assemblages of public data have copyright in that collection, and:
2. Such assemblages may be created automatically by a computer and still retain a copyright.

So if an organisation or organisations make the effort to collect data about you that can be linked via intrinsic identifiers in a digital form, not only will they own the digital form of the identifiers but also the full set of tokens the comprise your digital identity.

The Government asserts copyright over public information and extracts a monopoly rent for it². How profitable it will be to own peoples own digital identity. As this is clearly what is implied by the current database and copyright law....

In a real sense you will then not own your own identity. A highly valuable commodity, as

¹ http://www.wto.org/english/tratop_e/trips_e/trips_e.htm (accessed October 4th 2007)

² This is a regular complaint in Australia about collections of data made and held by the Australian Bureau of Statistics, and in the UK about the holdings of mapping data by the Ordnance Survey – where they have attracted a widespread “give us back OUR data” movement.

identity theft is now demonstrating. Only here it is not the transaction done in your name- but the very data that comprises your own identity that is alienated from you. The potential for this outcome was discussed at the time of the TRIPS negotiations by Wigan (1992).

9 Conclusion

The growing use of digital identifiers takes on a very special set of social impacts if collapsed by the wide use of biometrics and especially with ID cards linked to biometrics, however unreliable.

Once identity becomes the presentation of a digital dataset, then the very ownership of ones own 'identity' then comes into question. While this may not prove to be a problem, the collapsing of our daily multiple identities into one has far wider implications than are immediately obvious. This paper has simply introduced a few of the Implication.

The term uberveillance is correctly applied to the combination of powers and asymmetries and consequences of these trends.

References

Brin, D. (1998). *The transparent society*. Addison-Wesley, Reading Mass.

Clarke, R. (1994). *Human Identification in Information Systems: Management Challenges and Public Policy Issues* <<http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html>> (accessed 4 October 2007).

Independent Commission against Corruption (1992). *Report on the unauthorized release of Government information*. ICAC Sydney.(3 volumes)

Staples, W.G.(1997). *The culture of surveillance: discipline and social control in the United States*. Contemporary social issues series [Ed. G Ritzer], St Martins Press, New York.

Wigan, M. R. (1992). Data ownership. In R. A. Clarke & J. Cameron (Ed). *Managing information technologies, organisational impact II*, 1 (pp. 159-169). Amsterdam, North-Holland