Identity Policy: Risks & Rewards

APRIL 2007

Report prepared for the U.S. Federal Trade Commission

WRITTEN BY

Simon Davies and Gus Hosein

Policy Engagement Network,

Information Systems and Innovation Group,

The Department of Management, LSE

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Table of Contents

Introduction

The United States has initiated a number of actions and activities that have led to an increased focus on identity. Though this is an emergent area of interest, there have been a number of earlier activities and initiatives throughout the world that now act as the building blocks for current thinking about how to approach the creation of a coherent identity policy.

The aim of this paper, prepared by the London School of Economics and Political Science (LSE) at the request of the U.S. Federal Trade Commission, is to present and to discuss the international experience in establishing identity policies, and to set out a range of options that might be considered at this early stage. The paper also discusses the process options that should be considered as the nation moves forward in the identity dialogue.

While the FTC's work in this arena is focused primarily on discovering solutions to identity theft it is important to recognise that any emergent technology or policy in the field of identity theft protection must have regard to application in a much broader environment. Equally, the interplay of broader aspects such as the Social Security Number or legal liability gives rise to the need for careful analysis at an international level.

In preparing this paper we have drawn upon the authors' own recent work on opportunities for identity systems for the UK Government, research on identity policy challenges funded by the Canadian Federal Privacy Commissioner, and collaborative work with a range of global private sector companies. We also review research conducted at an international level by a range of other organizations.

The identity realm is complex and rapidly evolving. Countless generations of credentials have already been issued by governments, companies and other organizations, usually in the form of identity cards, security passes, memberships cards and passports, often reliant upon some form of identity verification and vetting processes that use biographical, biometric and/or other personal information. The growth of computing gave rise to renewed concerns regarding authorization rights and profiles, linking roles with privileges. Combined with the spread of computer networking issues, renewed interest in authentication emerged as more people focused on how individuals could assert their rights within these privileges.

With concerns about financial, national and commercial security, all stakeholders needed to find a solution to the problem of confidence. How can confidence in our transactions be ensured in the age of global communications, travel and trade? Since the 1990s there has been a flurry of activity at the consumer, business and government levels to deal with the issue of identity assurance to ascertain the level of confidence one needs in a claimed identity for a specific context and transaction. In a number of countries this led to coalitions of government departments, business and consumer groups working together to look into how credentialing, identification, authorization and authentication could work across multiple systems and business contexts. Working together towards a national identity infrastructure could prove beneficial to all these parties, and has led to confidence-enabling policy regimes and standards across the world.

The creation of an identity policy is a significant investment of time and resources that has the potential to create benefits at an economic level and even to facilitate certain benefits at a personal level. Yet some identity policies are fraught with complexities, risks and challenges. Identity policies may reshape for better or worse the relationship between a government and the people. The risks are significant and there are few opportunities for a 'second chance' at establishing such a policy.

There are many paths forward, whether through policy or technology design, but not all identity systems are designed equally. There may be a way of achieving policy goals, satisfying driving principles (and the interests of the actors involved), while minimizing the harm to the relationship between the individual and the government, and also applying, preserving and enhancing privacy. This paper seeks first and foremost to identify options that meet these conditions.

Emerging Identity Policies

It is highly likely that the U.S. federal government will need to consider establishing an identity policy. But identity policies are also emerging on local levels, and even in the voluntary and private sectors. Developing a policy regime to recognize, standardize and create coherence amongst these policies is not trivial. In fact, the government may need to consider creating a policy framework for managing multiple identity policies.

A comprehensive identity policy involves creating or adapting a program for the collection and processing of individual-specific data that will be shared across services, both within and beyond government, often for a variety of purposes. Taking this broad definition of an identity policy, it is increasingly apparent that there are a number of programs in development across the U.S. that will constitute the core components of a national identity policy framework.

Some emerging components of an identity policy include:

- Western Hemisphere Travel Initiative: This initiative involves the use of ‘secure’ travel documents at sea, land and air borders. This will involve the collection of biometric and biographical data, and will also involve the development of greater data-sharing capabilities between border agencies in the United States, Canada and Mexico.

- e-Passport: In accordance with international standards emerging from the International Civil Aviation Organisation (ICAO), the State Department is implementing new passport standards to incorporate facial biometrics.

- REAL ID: This, and other initiatives of this type, attempt to ‘secure’ documents such as driver’s licences in order to limit their availability to some sections of the population (e.g. illegal immigrants) and to create an audit trail of ‘foundation documents’ to aid the validation of the issuance process.

- Voter management: There are a number of state-level initiatives to reduce perceived ‘voting crimes’, including false registrations through deceased voters on voter registration lists, multiple votes, non-citizens and felons voting, or voting in some else’s name.

- Know your customer rules: These initiatives, originally started with banks but are now spreading to other sectors, where private entities are required by law to accumulate personal information on their clients and to then profile these clients to note and report on aberrant and possibly illegal activity.

Indeed, there are serious policy choices to be made, and these must be considered with great care. Every shift in design and decision over specification will have significant ramifications. Identity policies, as with all sophisticated and complex policies, have contentious components:

- technological (e.g. will the program be centralized and on-line; or decentralized and off-line; permitting one-to-one verifications or one-to-many verifications?)

- legal (e.g. will there be an increasing duty to carry or a duty to be identified?)

- political (e.g. who is responsible for the policy? how will it be decided? who will (not) be involved in deciding?)

- social (e.g. will people trust and appropriate the policy and the technology because it is designed for their interests and enhances privacy or will it be seen as another mechanism for the government to collect more information on its citizens?)

Each of the policy choices carries significant risks. But the greatest risk is that the decisions we make (or choose not to make) may transform the relationship between the individual and the government.

This point was noted previously by the 2003 report from a Canadian Parliamentary Standing committee that was charged to look into the case for a national identity card for Canada. When the Committee questioned why identity cards are so contentious in the few countries without cards when most other countries already have them, they found that the issue hinged on the relationship between the citizen and the state.

> "The relationship between the individual and the state in Canada, the U.S., the U.K. and Australia was also discussed as a commonality that distinguishes our countries from those with a long-standing tradition of national identity card systems."[1]

Since that time, proposals for national identity policies have been considered in each of these countries. Lessons have been learned and significant challenges have emerged.

Greater understanding and knowledge is required as we undertake a deliberative process to establish identity policy. Failing to do so will be costly and will damage public confidence. We have already witnessed a number of policy initiatives moving forward with little discussion and without any broader consideration of the challenges that exist. This not only gives rise to concerns about democratic process, but also creates a situation where appropriate policy alternatives may not be considered.

[1] Interim Report: A National Identity Card for Canada?, Report of the Standing Committee on Citizenship and Immigration, October 2003.

Dynamics of Identity Policy

Like most policies that involve advanced social, legal, technological and economic issues, identity policies are complex. Here we identify some of the challenges that are likely to emerge as identity policies are decided upon.[2]

1. Political risks

The greatest risk created by any identity policy is political. That is, as with all policies involving personal data collection and processing, an identity policy hinges on public trust.

In almost every country when a national identity policy is first introduced, such as the Australia card in the 1980s and the UK Identity Card in more recent years, public support was initially quite high. In both Australia and the UK public support was above 80% at the time the proposals were introduced. As the proposals attracted debate and scrutiny, problems and concerns were identified. The political and media process followed and support eventually fell away. In the case of Australia support fell to around ten per cent while in the UK support fell to 45-50%.

These are not isolated instances. The French Government encountered opposition to its efforts to make cards machine-readable. German authorities have encountered public and constitutional barriers in establishing a national numbering system for the German identity card. The Philippine identity card ran aground in 1991 and again in 2006 because of cost and constitutional factors that were made public through a campaign of opposition by human rights groups. The New Zealand public also opposed the Kiwi Card, which was subsequently abandoned. In the late 1980's the government of Ireland abandoned plans to establish a national identity system.[3] The then Data Protection Commissioner for Ireland, Donal Linehan, objected vehemently to the proposal. While acknowledging the importance of controlling fraud, the Commissioner observed that the proposal posed "very serious privacy implications for everybody".[4]

Vendors and governments have tended quite naturally to focus on deliverables, costs and practicalities of an identity system. The perspective of the public can be substantially different. Opposition to identity systems can have no regard to promised benefits of a proposed system. That is, arguments opposing an identity policy often cannot be "balanced" against competing claims of increased administrative efficiency or cost savings.

[2] This section builds on our research to date into identity policies and programs in a number of countries. For more information please see 'Identity Project Report', the London School of Economics and Political Science, June 2005, http://identityproject.lse.ac.uk.

[3] Announced in the 1989 - 1993 Programme For Government document.

[4] Commissioner's Annual Report, 1991, p.2, 42.

It may be useful at this early stage to summarize the positions held by civil liberties and other groups that over the past twenty years have (often successfully) challenged the concept of a national identity scheme.

- Many of the claims made for the technology behind identity systems cannot be sustained. The justification advanced for some elements of identity policy may in some cases be well intentioned, but can to be based more on emotion and rhetoric rather than credible research.

- The cost of the identity system, together with appropriate registration procedures, IT infrastructure, private and public sector compliance and parallel systems are likely to be well in excess of initial estimates.

- The privacy threats arising from a national identity system cannot be overstated. An identity system in any legal environment may fundamentally violate the privacy principles enshrined in law.

- Despite appearances to the contrary, there is little or no evidence in the research literature to establish that identity systems either significantly reduce the threat of terrorism or reduce the incidence of serious crime. Indeed the establishment of an identity system requires the creation of a new range of offences, and introduces the very real threat of increased criminality in a number of realms.

- Patronage of the idea of an identity system is often pursued with little quantifiable evidence of the claims made for such policies. The presumption, for example, that a national regime can reduce illegal immigration, diminish fraud, assist national security or improve administrative efficiency may be entirely instinctive. There is little, if any, international evidence that an identity system can achieve more than a fraction of the goals set for it.

- Rights advocates have consistently argued that not only will such initiatives turn nations into more authoritarian societies, but they will fundamentally change for all time the relationship between citizen and state, the nature of government and the character of the nation.

- A national identity system often involves the concept of converged or "joined-up" data resources. This poses significant threats to the security of data and the privacy of the individual. It also introduces the inevitability that data will be lost, misinterpreted, mutated or abused. Multiple-agency access to sensitive data greatly increases the potential for misuse of information, either through corrupt disclosure or lapses in security.

Even in countries with long-standing national identity schemes, public trust remains a strong factor that restricts change. Recent plans to 'modernize' the French identity card scheme were put on hold after consultation when numerous problems were identified, with particular emphasis on how the proposed scheme would create a new social contract between the citizen and the state.[5] Nor are all identity systems equal: the UK scheme is the only one to propose a central on-line register with multiple biometrics as such a design would be considered politically unpalatable elsewhere. In Ger-

[5] ‘Project de carte nationale d’identite electronique’, un rapport part Le Forum des droits sur l’internet’, 16 juin, 2005.

many, for example, such a scheme would be illegal due to laws passed in 2002 that prevent the establishment of biometric databases.

One way by which governments seek to avoid this political risk is through the claim that the new policies are due to international obligations, or obligations established beyond the jurisdiction of the government that is introducing the policy. This is a common strategy that uses the introduction of biometric travel and border documentation as a platform for introducing changes to identity policies even in those countries with existing national schemes. The UK is introducing its first peacetime identity card on the grounds that much of the infrastructure to deploy a national identity card is already being established due to U.S. and EU 'obligations' to enhance the UK passport through the use of biometrics. This policy strategy of displacing responsibility for a policy is also being used in the U.S. with the REAL ID Act where states have reduced powers to question the federal statute.

These strategies are successful only to a certain extent. We have already seen controversies arise in the U.S. where some states have rejected the implementation of the REAL ID Act's provisions within their jurisdictions. With biometric passports governments are now realizing the political problems that are emerging from a poorly-debated policies of fingerprinting (e.g. how do we secure fingerprint data?), and new enrolment strategies (e.g. how can the mass registration of the population be made viable?). All these activities will likely give rise to significant political risks as the realities of the schemes become evident.

British Prime Minister Tony Blair conceded this perspective in a speech he gave to News Corp in July 2006. Despite having successfully passed the legislation through the UK Parliament, though after a near-constitutional crisis brought upon the government by a recalcitrant House of Lords, he admitted:

> "It is, to me at least, almost incredible that the proposal to introduce an identity register in the UK should be so extraordinarily controversial. But it is."[6]

Even to this day support for the card hovers at around 50% even before a single card has been paid for or issued, and there is an even more significant lack in confidence that the government can successfully deploy the scheme.

The political risks in the U.S. are substantial. Research from Queen's University[7] in 2006 found that support for identity policies varied considerably around the world. For instance, 78% of French respondents agreed that everyone should have a government-issued ID card that must be carried with them at all times (with China falling behind at 77%). In Canada support was significantly lower, at 53%. The U.S. produced the lowest level of support, with only 42% supporting a national scheme. This is not a promising position for a national policy because, as we mention above, support for an

[6] Speech to News Corps', Tony Blair, Pebble Beach, California, July 30, 2006.

[7] David Lyon, Elia Zureik, and Yolande Chan, 'The Surveillance Project and the Globalization of Personal Data, available at http://www.queensu.ca/sociology/Surveillance/

identity policy tends to start quite high but then falls significantly as the public and policy-makers learn about and consider details of the plans. Unlike Australia and the UK, the U.S. is starting with a relatively low level of support, rendering any potential policy as being politically risky.

Another reason why strong surveyed support should be treated with caution is the question of how the relationship between the citizen and the state may be altered, even years after the initiative. Although France has a strong acceptance rate for its ID card, the issue remains a source of tension. Racial disquiet and tensions between minority communities and the police lead to the riots in 2005 in the suburbs of French cities. With a national election approaching, the police union, Alliance, revealed that officers were under orders to perform fewer identity checks to avoid raising tensions.[8] There are many reports around the world of minorities being disproportionately targeted by police using their stop-and-search powers for identity checks, leading to further political troubles.

Another key political issue is the confidence that citizens have in their governments to manage their personal information. When asked whether their own government will protect their personal information, the Queens' University research found that only 38% of Americans agreed (while most other countries had significantly higher support e.g. Canada (48%), China (63%); while Brazil had even lower support (20%)). One conclusion that may be drawn is that Americans are not aware of or confident in the laws that purport to protect their personal information. These numbers would likely fall, therefore, if Americans' faith in their personal privacy were to be tested through an identity policy initiative involving significant data collection.

It is possible that through these backdoor mechanisms the policies will slowly become adopted and accepted by Americans, as they grow to be a part of the daily lives of citizens in countries with extensive identity systems. But a policy initiative that relies on complacency as an adoption strategy is inadvisable, and potentially politically dangerous. Citizens are often adept at noticing initiatives that are ambitious and wide-ranging, particularly when they apply to the entire population.

2. Drivers

Identity policies are often introduced as an inevitable outcome of the spread of e-government, international obligations, requirements to combat fraud and terrorism, and other such drivers. We therefore need to scratch beneath the surface to better consider why governments introduce changes to identity and information management policies and practices.

In our research and experience, modern identity policy proposals rely on a limited number of arguments from proponents, including amongst others:

[8] 'Battle of Gare du Nord rocks Paris', Henry Samuel, Daily Telegraph, March 29, 2007. One of the leading candidates for the election is the former minister of the interior.

- the need to combat terrorism (e.g. the UK government argued that a third of all terrorists use multiple identities; REAL ID was implemented as a recommendation from the 9/11 Commission)
- the need to combat fraud (e.g. to ensure that only those who are entitled to government services may actually receive them; to limit voting to those who have the right to do so)
- the need to manage borders (e.g. the implementation of biometric visa schemes and to combat illegal working)
- the need to combat identity theft (e.g. the growing concern about fraudulent use of identities to open accounts in other people's names)
- the need to support the private sector with an adequate regime of identification (e.g. to enable the travel and finance sectors to verify the identity of their clients)
- the need to aid the development of electronic government services (e.g. to enable citizens to gain access to government services on-line will require some form of authentication in order to file taxes, etc.)

These are all valid reasons to reconsider existing identity practices, though it is daunting to consider them all within a single policy. An open and deliberative policy process requires additional information to inform decision-making so as to best understand the type of system(s) to develop. For instance, if the over-riding goal is to adhere to international obligations then this will have deterministic effects on the form of the policy: it will involve the use of biometrics and contactless chips that contain specific and limited information regarding the individual, in accordance to international standards from United Nations bodies.

But if the purpose is to combat fraud and identity theft the nature of the policy solutions differ significantly. We first need to establish the extent of these problems to better contemplate if these drivers should be the primary consideration for the design strategy. Is fraud really a serious problem, and can a changed identity policy possibly solve that problem? Or are new challenges being introduced by such changes? For instance, a growing reason for establishing identity policy is to reduce voter fraud. State laws that require identity documents for registration and voting have become controversial. Cases have shown that this approach could exclude significant sectors of the population. According to reports, at least 11 percent of voting-age Americans, disproportionately elderly and minority voters, lack the necessary papers.[9] Other research has found a lower voting turnout in jurisdic-

[9] 'The myth of voter fraud', Michael Waldman and Justin Levitt, Washington Post, March 29, 2007.

tions with these identity requirements.[10] This is despite emerging evidence that there are no clear systemic problems with voting fraud.[11]

Identity systems are not all built equally. They must be designed for specific purposes. We have seen a number of policy processes where the driving principles of a scheme have shifted in mid-course and this dynamic has raised the political risks of the entire scheme, particularly as information is released to the public and people begin to feel as though they have been duped into believing the policy is necessary, only to later conclude that this may not be the case. The haemorrhage of support in the United Kingdom emerged as the UK government shifted its arguments from terrorism to identity fraud, and supported its case through 'evidence' of the extent of identity fraud that was subsequently identified by the media as being 'inflated to play on public fears'.[12]

3. Feasibility of Goals and Realities

Once the driving principles are adequately established a government and key stakeholders need to be certain that the scheme can in fact be developed within realistic timelines and with reasonable technologies. Can the system in fact be built to fulfill the stated goals and objectives?

For instance, to ensure that fraudulent identities could not be created, governments are increasingly arguing that biometrics should be collected and stored in a central database. But if this is truly the function of the system, the technological implications are substantial. Can the biometrics of an entire population actually be enrolled with sufficient accuracy to prevent re-enrolment by fraudsters? That is, upon registration the register would be queried to ensure that the individual had not previously registered those biometrics. To this day we are still unsure whether biometric technologies are adequate to this task, even though a number of countries are moving to widespread deployment.[13] Similarly, to reduce the fraudulent use of biometric identity documents, the document-holder would need to have her biometrics scanned at every point of use. We are uncertain of any successful widespread deployment of such a system.

We need to ensure whether it is realistic to rely entirely on the creation of a new scheme. Recently the UK government announced a shift in its strategy and decided to create the register by way of building on top of existing databases and data sources. While such a scheme is far more feasible from the technological point of view it calls to question the original promises made to Parliament that the identity register would be a fresh database that would not inherit the data integrity problems from earlier databases that are likely to have erroneous data and multiple registrations. If we do not intro-

[10] ‘Lower voter turnout is seen in states that require ID’, Christopher Drew, the New York Times, February 21, 2007.

[11] ‘In 5-Year Effort, Scant Evidence of Voter Fraud’, Eric Lipton and Ian Urbina, the New York Times, April 12, 2007.

[12] ‘ID fraud figures inflated to play on public fears', Richard Ford and David Charter, The Times, February 3, 2006.

[13] ‘Home Office advisor urges biometrics testing', Tom Espiner, ZDNet UK, October 20, 2006 and 'Untested ID cards tech to go live', Steve Ranger, Silicon.com, October 23, 2006.

duce a significantly new system then we need to consider the political risks of bothering at all if the same problems may continue, even if it is likely to be at a reduced scale. This is particularly so when the political process relies on promises of radical reductions in social problems.

Generally if a new policy is to build on an existing identity infrastructure and offers innovations such as the inclusion of audit trails for the enrolment process (as is required by the REAL ID Act) or additional biometrics (as is the emerging strategy across Europe) these policies will encounter similar problems as those identified in the UK. These shifts in existing infrastructures may not result in sufficient reductions in the problems that were originally identified and again will create scepticism as to the purposes of the policy.

There will also be a legacy problem. For instance, while the U.S. State Department began issuing ‘biometric’ passports to U.S. citizens, involving a digital photograph of the face, it will take up to a decade to position the entire passport-holding population in the U.S. to use the new system. This leads the public to question the purpose of the introduction of additional measures to regulate access to the service if the existing mechanisms are still adequate. Similarly, former commissioners of the INS recently called for biometric social security cards. Because of the employment of illegal immigrants who fraudulently use social security cards, they argue that ‘replacing old cards over a designated period would resolve the problem on a national scale’.[14] The scale of such a registration process of all U.S. citizens is, for a lack of further research, unimaginable.

This 'reality-problem' has many dynamics. For instance, a new system is unlikely to induce any large-scale benefits until a significant portion of the population is enrolled. But the population will not enrol until it is required to, which is usually at the point of expiration of an older credential. This leads to a slow enrolment rate, which does not provide enough incentives to agencies and other potential 'users' of the system to adapt their own systems to the new identity system. For instance, banks will not start buying new chip-readers until enough individuals hold chip-based cards. But the lack of applications for the credential doesn't create sufficient incentive for people to sign up at an early stage for the new credentials. If the government were to then compel large populations to sign up, e.g. changing the border requirements for air travel to require passports for U.S. citizens returning from Canada and Mexico, the enrolment-infrastructure would have to deal with a massive influx of applicants, which will then cause queues and delays, thus inconveniencing the population. Recently this exact situation arose, where passport issuance processes have been hit by long delays, from 6 weeks to 10 weeks, leading to complaints being sent to members of Congress.[15]

The alternative is to introduce a mass enrolment into a new scheme though what is called 'the big bang approach', as is being considered in Australia with its new smartcard. The Australian govern-

[14] ‘The Winning Card’, Doris Meissner and James Ziglar, The New York Times, April 16, 2007.

[15] ‘U.S. warns of long delays for passports’, Matthew Lee, Associated Press, March 16, 2007.

ment plans to require the entire population to register for a new card within two years of the project going live. The new card would then expire every 7 years. This means that while the entire population would have to attend registration centres to get a new card within years 1 and 2, between years 3 and 7 these registration centres will be relatively empty as staff and buildings await the return of those who registered in year 1 as they return for their new cards in year 8. Such a policy design would be quickly ridiculed as an ineffective use of public resources, and again, will introduce political risks.

4. Effectiveness of the Choices

Even if a system can be built within the existing technological capabilities we still need to ask whether this is the appropriate design specification to meet the specified goals, or whether it is merely introducing additional challenges.

In the United Kingdom, industry and government experts stepped forward to criticize the centralized design approach for fear that it may introduce additional vulnerabilities. That is, the government's national identity scheme was criticized for its use of a single register that will store a large amount of sensitive information and it would provide the ideal opportunity for identity fraud on a grand scale through infiltration of the register.[16] Similar criticisms have been aimed towards driver's licensing authorities in the U.S. who now have to hold even more information on their drivers because of the REAL ID requirements.

The European Union and the U.S. both encountered this risk after they introduced changes to their passport regimes. The EU decided to create a regulation requiring all EU member states to implement a biometric passport using fingerprints. This circumvented national parliaments debating the merits of the proposal. After moving the policy through the European Parliament, policy-makers noticed that the inclusion of fingerprints in passports would mean that whenever EU citizens travel to other countries outside of the EU then these countries would by default be able to access the fingerprints of EU citizens even though this access may not be a requirement. The EU eventually had to introduce a band-aid fix through the use of encryption. Similarly the U.S. discovered that contact-less chips would communicate the personal details of U.S. citizens without their consent, identifying U.S. citizens while they travel abroad. This generated significant public concern and the U.S. had to adopt a patch for this problem through introducing basic access controls. All these patch-solutions decreased public confidence in the policies.

Often information-sharing is seen as a promoter of new identity policy, but this approach at a number of levels is not easy to manage. The UK government initially decided on developing an entirely new identity infrastructure instead of building on existing identity mechanisms and policies. The problem

[16] 'UK ID card a recipe for massive ID fraud, says Microsoft exec', John Lettice, The Register, October 18, 2005.

is that this would have required every government agency and every private sector partner to redesign their databases and their processes to deal with this new identifier, often on top of their existing identifiers. In the U.S. context, this is equivalent to issuing a replacement to the Social Security Number, and then requiring every state agency and private sector firm to change their computer systems to accept the new numbering system. This will introduce significant political problems, as every other government department would have to find the resources and the willingness to introduce changes.

There are other approaches to this problem. While the French government's justice department considered the creation of a new identification card with a centralised citizen-register, another French government department was arguing for a more decentralized option through the creation of a 'card-wallet' that would permit individuals to hold a card that contained multiple identifiers, each one relevant to each government service they used. So, for example, the existing health-card identifier would be placed on the new card; but this information would not be relevant to the pension-department as that department has its own unique identifier used in its own systems. Accordingly, that unique identifier would also be placed on the card-wallet. Such a decentralized scheme raises its own feasibility problems because we need to better understand who would govern the system and whether this is consistent with the political goals in introducing changes to the existing practices and schemes. Finally we would need to ask whether such a scheme justifies the creation of a new policy if it is merely a band-aid on top of the existing infrastructure. But this divergence in approaches shows that there are a number of policy options that lead to different system designs.

5. Costs

Nearly all stakeholders in any debate on identity policy agree that there is probably a need for some form of innovation to meet the noble goals outlined by proponents of policy change. However, when the policy is brought forward there is often an over-riding concern whether the resulting system is cost-effective.

This is not to mean that we should let costs be the primary concern when considering the deployment of a new identity policy. But as with all matters of public policy we must ensure that burdens are at the very least commensurate to the gains, and that the approach is politically palatable to the affected audience. In this case, the 'affected audience' is a combination of government, industry, and the general public.

There are at least four facets of costs-consideration: costs attributed to design decisions, management of costs, opportunity costs, and cost burden.

Costs are immediately incurred due to design considerations. In the United Kingdom a significant component of the costs within its scheme are due to choices in design. To prevent multiple enrolments, the scheme requires collection and processing of multiple biometrics, each of which incur significant costs (iris scanning being the most costly at the moment). The centralized register also incurs costs particularly because of its purpose of combating identity fraud - every use of the card would have to be checked against the central register to ensure that the card is valid, and perhaps an additional biometrics check to ensure that the holder is who he says he is. The implementation of untested technologies such as contact-less chips, combined with their widespread use, may incur additional costs due to a reduced life-time of the card. For example, current British passports have a 10-year expiration but this could be reduced due to wear-and-tear on the cards and their contact-less technologies. A UK National Audit Office report recently found that the new chips contained in the passports had only a two-year warranty.

Similarly, the reduced lifetime of the biometric technologies may also be problematic, as technologies evolve and as people age. Enrolment centres will have to be geographically dispersed in ways that they are not currently structured because people are accustomed to renewing their identity documents by sending them to the responsible department by mail. This was probably one driving consideration for the U.S. Department of State in their rejection for the time being of fingerprints in the U.S. passport: fingerprints, unlike facial biometrics, must be registered in person at an office using specific technologies, and the State Department does not have such a geographic reach. Therefore, every design consideration and every additional purpose attributed to the system will create a ramification on the costs of the scheme. Far too often we see ambition replacing reason within the policy design stage, and the effects are only felt later as governments and industry sectors try to fund the systems that countries have been promised.

The management of costs is also significant. That is, which government administrative department will pay for the scheme? In the United Kingdom the interior ministry, the Home Office, was behind the introduction of the Identity Cards Act. In its regulatory impact assessment the Home Office contended that the scheme would only cost 584m pounds (approximately 1.1 billion dollars) per year to administer, and this was then rounded to £5.8bn (eleven billion dollars) over ten years. Contending estimates were in the range of £7 to £19bn over ten years and led to significant public controversy. Eventually it emerged that the Home Office's estimate only catered for the costs to the Home Office to administer the scheme (and even then, only a few departments in the Home Office) rather than the government as a whole. So while the purpose of the card included reducing benefits fraud, the £5.8bn figure did not cater for the costs for the Department of Work and Pensions or the Department of Health to integrate the system into their operations and procedures in order to combat welfare fraud. The same applies for the police, border officials, and so forth.

Similar dynamics emerged in the U.S. where the REAL ID Act is now seen as an unfunded mandate. That is, the federal statute requires each state to introduce changes to their driving licence issuance process, to the security of the card and the sharing of data about each card-holder. Congress did not fund this initiative and instead left it to each state to implement and fund. This has generated significant concerns across the states with repeated objections to the law from organizations such as the American Association of Motor Vehicles Agencies (AAMVA), the National Governor's Association and the National Conference of State Legislators. In a report released jointly by these organizations, state motor vehicle officials estimated it would cost more than $11 billion over five years to implement the technology required by the Real ID Act, while an earlier Congressional Budget report had originally envisioned costs would be in the range of $20 to $100 million.[17] Now the Department of Homeland Security has estimated costs to be between $17 and $23 billion over the next ten years.[18]

A common – and usually accurate - political strategy for those who oppose identity policies is to question whether the costs for the scheme would not be better spent elsewhere. This strategy is very successful at reducing public's confidence in the policy, again returning us to the political risks of identity policy. Accepting that these policies tend to be quite expensive, critics point to the 'opportunity costs' introduced by the scheme. That is, these funds might be better spent on other government programs. This was one of the leading strategies in the Australian and New Zealand debates in the 1980s where it was argued that the funds should instead be spent on health. In the 1990s in Britain, while leader of the opposition, Tony Blair questioned the Tory's proposed identity card on grounds that the money is better used in policing.

Another related strategy questions whether alternative and existing mechanisms aren't already sufficient and may be improved for a fraction of the cost. For instance, while the UK identity card could help employers enforce legal requirements to verify the immigration status of employees, this process is already possible as all foreign employees are required to hold visas and passports that are verified and logged by employers. Instead, critics argue, the government is doing an insufficient job of applying existing measures and laws even as they consider new ones.

Finally, another facet to the costs issue is who will actually have to bear the costs of the scheme. While these schemes may be generally expensive, governments are reluctant to bear the full brunt of the costs. There are two predominant strategies used to share the burden, and one emerging strategy. First, as was done in the Netherlands, the government requires that citizens carry identification papers at all times but does not mandate which form of identification this should be. At the same time, the government offers a 'voluntary' card that citizens are required to purchase. This way the government avoids introducing a perceived tax. A second strategy is to increase the costs of issuing existing documentation, as is done in the UK, where in order to implement the biometrics required for the identity card the price of passports will nearly double in the period between 1999 to 2009. By so doing, citizens do not feel as though the card itself is too costly because they accept that the pass-

[17] 'ID Program Will Cost States $11 Billion, Report Says', Darryl Fears, Washington Post, September 22, 2006.

[18] Department of Homeland Security, Notice of proposed rulemaking: Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, March 2007, page 106.

port is a document that they have always paid for. Finally, an emerging strategy, again from the UK, is to charge the private sector and other government departments for their use of the card and the associated national register. Every time a bank, telephone company, or even local government agency queries data on the register or reads the card, they will be required to pay a transaction cost (currently estimated between £0.50 and £2.00 or between one dollar and four dollars). If there is sufficient buy-in (possibly enforced through regulation) then these verification-transactions can generate significant funds. The UK government estimates that eventually more than 260 government departments and 44,000 private sector organisations will want access to the register, resulting in an estimated 163m transactions per year.[19]

All these cost dynamics will have significant ramifications on the political risks to the identity policy unless carefully considered.

6. Who decides the policy and owns the system?

Related to the issue of costs management is the issue of policy-ownership. Whoever has ownership of the policy will likely have to deal with specific political, design, and cost risks.

We have already noted the problems with REAL ID and who actually owns and pays for the policy's effects on systems and practices. Even the choice of which government department will be responsible for the policy can also give rise to controversy. A policy introduced by a ministry responsible for immigration will give rise to concerns that the policy is designed to place immigrants under surveillance. There are also design considerations: a policy owned by the policing arm of government tends to be focused on policing; a policy from the Treasury tends to focus on managing employment and taxation. For instance, one of the reasons to include fingerprints in the UK identity card is because the Home Office is hoping to identify the 900,000 fingerprints that have been found at scenes of crimes over the years but not yet resulted in matches on the database of fingerprints of criminals. The scheme is thus seen as being designed for policing purposes rather than for administration of government services; and this may reduce confidence in the scheme as citizens are sensing that they are being treated like criminals.

The exact situation arose in the U.S. at about the same time. Even as the Department of State promising that the new biometric passport would not include fingerprints, in his outgoing speeches former DHS secretary Tom Ridge was calling for the inclusion fingerprints in U.S. passports.[20] "I think one of my recommendations to [current Secretary of DHS] Mike [Chertoff] is be aggressive, go after ten fingerprints on the passport." Yet again, two departments with different goals respond differently to design choices.

[19] Home Office presentation to industry, 'Procurement Strategy Market Soundings', Identity Cards Programme, Home Office, October 2005.

[20] Secretary Tom Ridge, 'Homeland Security: International Dimensions', Speech to the Center for Strategic and International Studies, January 12, 2005.

Of course it is dangerous to approach the design of the scheme in such a deterministic way of 'who owns it designs it in his interests'. But an interesting example of this situation emerges from France: when the ministry for state reform recommended a policy. It called for a federated scheme that would serve the interests of the citizen and the existing practices of each government department; but when the ministry of interior called for a new policy it recommended one similar to the UK Identity Cards Act with a heavy biometrics component, a single identifier and a centralized register.

7. How does the system regard privacy and civil liberties?

A predominant concern with the introduction of an identity policy is the risk it poses to privacy and civil liberties. For instance, to those who live in countries without identity cards, the very notion of being compelled to carry a card can conjure images of oppression and discrimination. Practically every government considers these issues within their policy, but how well they consider it in their design and implementation will influence the level of risk that is likely to arise.

The use of central registries with audit trails, compulsory registration powers, compulsion to identify, extensive use and re-use of personal data and biometrics, and the extent of user-control over the system are key considerations for privacy and civil liberties. Each policy weighs these components differently and this in turn has significant effects on the political risks. For instance, although Germany has a long history of national identity cards and is now implementing biometric passports it has restricted the storage of biometrics in a single register due to fears of abuse. The French and the British are interpreting the EU requirements differently by requiring between 8 and ten fingerprint images. Amongst others, Australia, Spain and the U.S. have rejected this approach.

The UK did offer an innovation to promote privacy: the creation of an office of the Identity Commissioner who would oversee the privacy implications for the scheme to ensure that there is no abuse. It remains to be seen if this will increase public confidence, particularly since the design of the scheme is the most invasive ever created with a central register that logs every verification in such a way that the audit logs will show every single transaction activated by the individual with that card (e.g. every time it was verified at a border, at a hospital, at a benefits agency, by a bank, etc.) and essentially mapping out many of the actions that constitute the daily life of an individual. The UK government contends that this approach will empower the citizen because individuals will be able to verify the audit trail to see whether a bank, benefits agency, or hospital has access his personal details, thus theoretically ensuring that there is no abuse. The outcome of this approach remains to be seen but the UK government policy does run a significant risk of being seen as privacy-invasive in ways that other countries' governments have managed to avoid.

Americans are said to value their privacy, and this has been validated through numerous polls and surveys. They are also quite concerned about the processing of their personal data. Identity policies are amongst the greatest recent challenges to promoting, enhancing and safeguarding privacy. Identity policies can enable or prevent the collection, processing and sharing of personal information across government departments, and even with the private sector. Considering all the other challenges and risks of identity policies, it is likely that privacy may yet produce the largest political risk in the U.S. context.

Crucial components of an identity scheme

When deciding upon and designing an identity policy it is, in our experience, not enough to merely affirm or re-state a commitment to the right of privacy or the supremacy of the individual. It is in our view more important to break the identity matrix down into component parts and present guarantees and options at every component level. Here we set out principles and foundations that have been used in the world's most successful and trusted identity systems. In doing so we have adopted the following assumptions:

- No national identification system is totally secure, nor can any system ever be immune to the risk of accepting false or multiple identities. Any such claim would not only be demonstrably false, but it would lead to substantial and sustained attacks. Biometrics can be spoofed, registration data falsified, corruption exploited and social networks manipulated. At both a human and a technological level, a fixation on achieving perfect identification across the entire population is misguided and counter-productive. Such emphasis is disproportionate and will lead to substantial problems relating to cost, security and trust.

- The choice of any national identification system should involve careful and sensitive consideration of key aspects of cost, security, dependability and functionality. This exercise is not necessarily a Zero Sum equation where the value of one element is traded off against the value of other elements. The aim of a genuine evolution of thinking is to achieve high scores on all key elements of the scheme. Only a spirit of openness makes it possible for this outcome to be achieved.

- Public trust is the key to a successful national identification scheme. Public trust can only be secured if issues of cost effectiveness, dependability, security, legal rights and utility are addressed, and which are seen to be addressed. We believe it is possible to achieve these goals while also ensuring a system that offers reliable means of achieving a range of stated objectives.

- A genuinely cooperative approach to finding a national identity solution must involve consultation based on principles as well as objectives. While a goal-based approach may provide short term political cover and satisfy key stakeholders involved in those specific goals, the approach imperils other essential aspects such as public trust.

We have identified a set of elements that should ideally guide the design and execution of a national identity scheme:

An identity policy must be proportionate. Aspects such as complexity, cost, legal compulsion, functionality, information storage and access to personal data must be genuinely proportionate to the stated goals of the ID system.

An identity system should be inspired by clear and specific goals. Successful identity systems embrace clear objectives that facilitate responsive, relevant and reliable development of the technology, and which limit the risk of exclusion and abuse.

Identification systems must be transparent. Public trust is maximized when details of the development and operation of an identification system are available to the users. Other than possibly the identifier and card number, no personal information should be hidden.

Identity disclosure should be required only when necessary. An obligation to disclose identity should not be imposed unless the disclosure is essential to a particular transaction, duty or relationship. Over-use of an ID system will lead to the increased threat of misuse and will erode public trust.

An identity policy should serve the individual. Public trust will not be achieved if an identity system is seen as a tool exclusively for the benefit of authority. A system should be designed to create substantial economic, lifestyle and security benefits for all individuals in their day-to-day life.

A national identity system should be more than just a card. Identity systems must exploit secure and private methods of taking advantage of electronic delivery of benefits and services.

Personal information should be controlled by the individual. Any biometrics and personal data associated with an identification system should remain to the greatest possible extent under the control of the individual to whom it relates. This principle establishes trust, maximizes the integrity and accuracy of data and improves personal security.

Empathetic and responsive registration is essential for trust. Where government is required to assess and decide eligibility for an ID credential, the registration process should, to the greatest possible extent, be localized and cooperative.

Revocation is crucial to the control of identity theft and to the personal security of individuals. Technology should be employed to ensure that a biometric or an identity credential that has been stolen or compromised can be revoked.

Identity numbers should be invisible and restricted. Any unique code or number assigned to an individual must be cryptographically protected and invisibly embedded within the identity system. This feature will protect against the risk of identity theft and will limit “function creep” through extended use of the number.

Capability for multiple authenticated electronic identities. An identity system should allow individuals to create secure electronic identity credentials that do not disclose personally identifiable information for use within particular social or economic domains. The use of these different credentials ensures that a “master” identifier does not become universally employed. Each sectoral credential is authenticated by the master identifier assigned to each individual. The use of these identifiers and their control by individuals is the basis for safe and secure use of federated identity systems.

Minimal reliance on a central registry of associated data. Wherever possible, in the interests of security and trust, large centralized registries of personal data should be avoided.

Permit secure and private backup of associated data. An identity system should incorporate a means of allowing individuals to securely and routinely back up data stored on their card. This facility will maximize use of the identity credentials.

The crucial factor: The Policy Process

The creation of public trust in an identity system depends on a sensitive, cautious and cooperative approach involving all key stakeholder groups. Public trust thrives in an environment of transparency and within a framework of legal rights. Importantly, trust is also achieved when an identity system is reliable and stable, and operates in conditions that provide genuine value and benefit to the individual.

These conditions will not easily be created. They must evolve through a clear, genuine and thoughtful policy process.

Our view, based on the international evidence, is that a appropriate identity policy for the U.S. would be one based on a foundation of public trust and user demand rather than one based solely on enforcement. The goal of public trust would be made possible, in part, through the use of reliable and secure technologies and the creation of a flexible "citizen centered" model.

Any successful, trusted, complex and sensitive policy requires five elements of process: Discourse, Deliberation, Decision, Design and Delivery – each of which is interconnected.

Discourse comprises the vital first stage in the policy process during which policy makers and key experts determine the objectives, necessity and the frame of reference for a potential policy initiative. This stage is crucial in that it establishes an intellectual, legal and moral foundation that will form reference points for subsequent stages.

Deliberation encompasses the majority of the public consultation along with stakeholder engagement and any necessary research work. A consultation process in a domain as potentially sensitive as identity should generate discussion, feed into the policy process, make individuals aware that they are part of the decision-making process and improve the quality of the policy through the solicitation of a wide spectrum of ideas, opinions, and facts. A true consultation process would solicit alternative views, schemes and architectures.

Decision is the weak link in most policy processes. A truly genuine and effective decision stage involves a structured approach similar to the ideal Discourse environment. It should involve the systematic consideration of all output from previous stages rather than using those stages as a mere device to justify a pre-ordained policy.

Design should be undertaken with regard to all previous stages, and encompasses a more clinical approach to the achievement of goals, targets and objectives. The Design stage should, wherever possible, be transparent and accountable.

Delivery is the final stage, and should be foreshadowed as frequently as possible in the Design phase. It is within this crucial element of the process that goals such as trust and broad take-up can be achieved, or where of course they may fail, setting the entire policy process back to phase one.

An analysis of effective identity policies across the world reveals that these five elements are integral to their very success.

About the Authors

Simon Davies

Simon Davies is widely acknowledged as one of the foremost privacy experts in the world, and is one of the pioneers of the international privacy arena. His work in the fields of privacy, data protection, consumer rights and technology policy has spanned more than twenty years. Simon is perhaps best known as the founder and Director of the watchdog group Privacy International, but is also an academic, consultant, journalist and author. Simon's interests cover the entire privacy spectrum, from identity systems, in-house data protection, government data systems and communications surveillance, through to the legal aspects of data protection. Simon has been a Visiting Fellow in Law at both the University of Greenwich and the University of Essex, and for the past ten years has been Visiting Fellow in the Information Systems and Innovation Group in the Department of Management at the London School of Economics and Political Science, where he teaches the MSc masters course in "Privacy & Data Protection".

Simon has advised a wide range of corporate, government and professional bodies, and has worked on technology, privacy and identity issues in more than forty countries. His work has put him at the forefront of numerous issues, including the debate over proposals for government identity systems, the ethics of CCTV surveillance, the development of encryption regulation, human rights law and the data trade between Europe and the United States. In April 1999, he received the Electronic Frontier Foundation's "Pioneer" award for his contribution to the development of the Internet. In both 2004 and 2005 Silicon.com voted him as one of the world's 50 most influential people in technology policy.

Gus Hosein

Dr Gus Hosein is a leading expert, researcher, and advocate on the intersection of technology, politics and civil liberties. He publishes leading research and reports regularly and speaks at dozens of conferences a year around the world. As a Visiting Fellow in the Information Systems and Innovation Group in the Department of Management at the London School of Economics and Political Science he has conducted research on technology policy, privacy, civil liberties and international policy-making. Since 1997 he has taught undergraduate and graduate students on information policy. He is a regular guest lecturer at academic institutions around the world and has previously held fellowships at Oxford University and Columbia University.

Gus is also Senior Fellow with Privacy International and works extensively with non-governmental and inter-governmental organizations. At Privacy International he co-ordinates research and advocacy on anti-terrorism policies, the activities of inter-governmental organisations, national and international identity and border initiatives, freedom of expression, and communications surveillance. He is also a Visiting Scholar at the American Civil Liberties Union. There he advises the Technology and Liberty Project on technology and civil liberties issues from an international perspective.

He holds a B.Math (Hons) from the University of Waterloo and a doctorate from the University of London.