OII Forum Discussion Paper No. 16

Towards a Policy and Legal Framework for Identity Management: A Workshop Report

by Mary Rundle

with assistance from Anna Dopatka

Oxford Internet Institute

University of Oxford

Forum Discussion Paper

Oxford Internet Institute

University of Oxford

1 St Giles Oxford OX1 3JS

United Kingdom

October 2009

This paper reports on discussions from a workshop organized by the Oxford Internet Institute (OII), University of Oxford, with the support of the Lynde and Harry Bradley Foundation. The Forum was held on 2-3 April 2009 at St Hugh's College, University of Oxford. It was convened by Mary Rundle, a Research Associate at the OII. She is an Identity Policy Strategist at Microsoft.

Contents

Introduction

An Oxford Internet Institute (OII) workshop, entitled “A Policy and Legal Framework for Identity Management”, was convened under the Free Identity project funded by the Lynde and Harry Bradley Foundation. The project’s mission has been to promote a legal and technological framework for identity management that safeguards the exercise of classical liberal freedoms – such as freedom of expression, freedom of association, privacy, freedom of religion, and protection for minorities – as people increasingly act through electronic identities. The project leaders acknowledge that governments are not necessarily united around these values. Nonetheless, the project has been designed with the expectation that, as a global infrastructure for identity management emerges, this infrastructure will require a greater alignment of legal systems in support of it, and that the process of alignment will uncover differences in regimes’ values. While the long-term hope is that universal human rights will be honored by all societies in the environment facilitated by the identity infrastructure, an immediate challenge is to learn how to craft policy and law for the identity infrastructure in ways that will support the values of free and open societies.

The idea for the workshop stemmed from an observation that a range of experts around the world have begun calling for a policy and legal framework to support an identity infrastructure, but to date there has been little cross-disciplinary dialogue to find out what people really mean when they issue such calls. Policymakers speak of legislation on identity cards; people in business point to uncertainties in liabilities; technology developers refer to the need for policy direction; and democracy advocates seek to safeguard privacy and other freedoms it enables. Given this wide-ranging set of viewpoints, the design of the workshop sought not to resolve the issues but rather to encourage thoughtful discourse on the evolution of a legal and policy framework to support an emergent identity infrastructure.

To set the stage for a roundtable discussion, the workshop began with short briefings from different stakeholder perspectives, including those of policymakers, business leaders, the technology industry, individual users, and civil society. Discussion then turned to connecting legal and technological issues, with a specific focus on international data protection principles and the workings of the envisioned identity infrastructure. In a use-case exercise, teams took on the values of different societies and applied data protection principles to specific points in the envisioned identity infrastructure. (See Annex I.) Participants then moved to an “open space” mode, where individuals could express their predominant concerns, and facilitators then clustered them for deeper discussion in break-out groups.

The entire group was reconvened for a roundtable discussion on the second day, where participants fed concerns and insights into sessions dealing with: the necessity of a policy and legal framework to support an identity infrastructure; whether or not such a framework would need to be global; how a framework could accommodate local values; the feasibility of any framework; and how a framework might be achieved.

This report provides an overview of the roundtable discussion. As the group was aiming not to establish consensus but rather to surface key issues, this synthesis has sought to reflect conflicting views as well as areas of relative agreement. To complement the report on this collective discussion, Annex III contains issue briefs written by many participants in advance of the workshop to highlight matters deserving more attention. Taken together, this material offers a preliminary stocktaking of some of the pressing issues that must be considered in the development of a policy and legal framework for identity management.

Is a Policy and Legal Framework *Necessary*?

An initial question when coming together to consider what would be desirable in a policy and legal framework is: "What are we doing and why?" In terms of the "what", it is useful first to start with an explanation of what is meant by "identity management" in the context of this workshop. In terms of the "why", it helps to consider different stakeholder interests, as these differences create the need for a policy and legal framework.

Aligning Conceptions

The meaning of the term "identity management" has changed significantly over the last decade. In earlier years, identity management was tied to enterprise management, focusing on how an enterprise could better manage customer accounts and personnel changes, including employees joining an organization, changing roles within the organization, and leaving the organization. In the 21st Century, identity management has come to connote not just access privileges, but also a systematic way of making assertions or claims about a person; at the behest of a user, identity providers may present these assertions or claims to service providers, who in turn may choose to rely on them (for example, payment information in an e-commerce transaction).

In 2009, it is useful to think of "identity management" as entailing:

- *Relationships* among parties involved in transferring identity information – including the "user" who is taking action to receive a service, the "service provider" or "relying party" that is doing something for the user, and the "identity provider" that stores the identity information about the user or "data subject" and transmits it as requested;
- *Attribute or claims transfers* containing identity information about a person – with this information including personal data that can be associated with a specific physical person, and/or information that cannot be tied to his or her physical person; plus
- The various *ways that transfers can be done* – with models including (i) "federated" systems, in which service providers use a central identity provider to authenticate the user and possibly to link the different accounts they each may have for that user, as well as (ii) "user-centric" systems, in which the user chooses which identity providers should store his or her information for transmission to service providers at his or her own request. This decentralized, user-centric model can allow for "multi-party security", whereby an electronic agent under the user's control is the only device containing all the links between a user's various "digital identities," or sets of identity information.[1] Employing the electronic agent and using cryptography, the user can arrange for claims to flow in a way that both enables service providers to trust that the claims come from a trusted third party, and prevents those service providers from linking up different transactions and creating a super, composite account of the user. (See Annex II for a comparison of models.)

Policy and law can apply to all these components. Workshop participants focused not on trying to spell out the full extent of policy and law that might apply or on imagining the many possible jurisdictional conflicts that could arise, but rather on *getting a sense of the types of interests likely to arise* that will need to be factored into a framework. The idea would be to lend predictability as to the rights and responsibilities of different parties, including (a) what are the different roles in relationships, (b) who has what control over attributes or claims, and

[1] The ability to prevent traceability is just one of 20 or so security and privacy features for users that fall under the umbrella of multi-party security. Moreover, untraceability is not fixed; the key point about untraceability is that each user can control the degree of linkability (and traceability) of his/her actions.

(c) what are the alternative ways that transfers can be conducted. Part of the task of providing this predictability would be to try to reconcile and accommodate the diverse stakeholder interests.

Stakeholder Interests in Having a Framework

Experts from different disciplines may carry preconceived notions of the problems and solutions for a policy and legal framework for an identity infrastructure. Dialogue across disciplines can help experts to appreciate the range of concerns that are vying for attention. This recognition can provide a more promising ground for defining a common conception across disciplines of what scope a framework will need to cover. For example, a technologist might begin with assumptions about the need for policy to spur common formats and schema, while a person from the financial sector might start with a desire for clarity as to which jurisdiction's laws pertain to an individual's bank accounts. By teaching each other about their respective frames of reference, people from different stakeholder groups can get a more complete sense of the range of needs that could be addressed in the policy and law supporting an identity infrastructure.

As an early effort to generate this interdisciplinary dialogue, the workshop brought out different stakeholder interests in policy and law relating to an identity infrastructure. By way of a distilled account:

Governments want policy and law to promote an identity infrastructure that enables them to serve their citizens more efficiently. On the lightweight end, they want to offer citizens an easy way to interact with agencies and departments. On the heavier end, they want to equip citizens with secure electronic identity documents (eIDs) to prove who they are, as a means for facilitating more critical transactions, such as crossing borders, accessing health records, or paying taxes. Government departments have a multitude of interests at stake. Some are focused on preventing harm, for example by countering terrorism or protecting citizens and organizations from malicious actors such as fraudsters. Still others try to reduce the effects of negligent behavior that can leave people vulnerable, for example by encouraging distributed data storage and encryption so the consequences are not dire if equipment containing personal data becomes lost. Other public interests include ensuring that the privacy of citizens is protected, and preventing individuals from being at the mercy of entities that have extensive profile information on them. As governments operate in regional and global settings, they want identity systems to interoperate internationally.

Companies, meanwhile, want to manage their employees' electronic access privileges and to tailor and personalize services for customers. In doing so, these organizations want to know they can comply with regulation, such as data protection laws; they would also like to see streamlined compliance requirements as they operate in multiple jurisdictions. They seek predictability to anticipate where they may incur liabilities and how they can mitigate risks. They also want to have a means of redress should something go wrong. Businesses are apt to want the identity infrastructure to recognize digital "juristic" or "juridical" persons (so that entities can enjoy rights the way natural persons can). Along the same lines, there may be demand for "limited liability personas."[2]

Besides business in general, there are particular businesses with key stakes in an identity management framework, such as buyers and sellers of personal data. Although there are some players in the world who are trading identity information for nefarious purposes, there

[2] See, *e.g.* "The Limited Liability Persona," entry posted by Bob Blakley on the Burton Group's Identity and Privacy Strategies Blog, 17 November 2006, at: http://identityblog.burtongroup.com/bgidps/2006/11/the_limited_lia.html

are quite legitimate buyers and sellers, such as marketing directors who are spending US$15billion on customer data, as well as the credit bureaus. These players must be in the conversation if a framework is to reflect the full ecology.

From the perspective of the individual user (the stakeholders at the heart of identity management), many people want policy and law to give them control over what personal information is shared and how it is used in different contexts. They increasingly expect to be able to use their identity information proactively. They want to enjoy “rich” experiences where content is customized to them and where they see interesting details about people in their social networks. More and more, their focus is on being able to *do* things. They want their identities to persist over time, for use at their discretion. People want to be able to port their identity information into new contexts. They may also want to have joint control over some digital identities. In these activities they want to have rights at least as strong as those they have enjoyed in the physical world. They also want to have a means of redress should something go wrong.

Given the potential gatekeeper role of this technology to determine whether people can act in the digital world, human rights and democracy advocates look to policy and law to shore up freedoms, for example by bolstering identity management systems that enable citizens to establish social networks and carry out peaceful protests. A key concern of these groups is for policy and law to protect people’s privacy and their right to be anonymous at times – with privacy and anonymity being not just ends in themselves, but also means by which people can enjoy other freedoms (e.g., political expression, assembly/association, religion) and enjoy other rights (e.g., protection for minorities) that might otherwise be thwarted.

Technology developers hope the needs of all the stakeholders above are met in policy and law so that customers will buy their products. Similarly, they want to design solutions that are appropriate to the legislative and regulatory environment that their customers will face, for example helping to reduce customers’ liability exposure. Hence technologists seek predictability in policy and law for product planning purposes. (So, too, at a directly technical level, policy and law could encourage certain technical standardization, e.g., for formats, schema, etc., that could help these products obtain network effects.)

Although the catalog above is highly generalized and could be easily expanded, it serves to illustrate both the diversity in stakeholder interests and the shared desire for predictability in rights and responsibilities as the information society relies on an identity infrastructure. Each set of interests is already complex when considered discretely; complexity grows when the sets of interests are taken in combination as a collection of potentially discordant concerns for a framework to reconcile and accommodate. While this endeavor may be daunting in and of itself, it arguably does not stop there: When the technical infrastructure spans jurisdictions, interests multiply, and the desire for predictability in rights and responsibilities becomes more pronounced. There may well be a need for a framework or frameworks to operate not just at a local level, but also at a global level.

The Properties of Identity as Indicators

Several workshop participants noted that the “Properties of Identity”[3] convey many of the challenges that negotiators of a policy and legal framework must address if they are to balance the interests of different stakeholders. The Properties of Identity appear in the text box below. Many of the key points that emerged from the Oxford workshop are related to one or more of these Properties of Identity.

[3] The Properties of Identity were presented in the OECD working paper “At a Crossroads: Personhood and Digital Identity in the Information Society,” DSTI/DOC(2007)7.

The Properties of Identity*

Identity behaves according to a number of observable properties, as follows:

1. **Identity is social.** Humans are naturally social. To engage in social interactions (including commerce) people need something that persists and that can be used as a basis for recognition of others – an “identity”.
2. **Identity is subjective.** Different people have different experiences with the same individual and therefore attribute different characteristics to that individual; that is, they will construct different identities for him.
3. **Identity is valuable.** By building a history of a person’s past actions, exchange of identity information creates social capital and enables transactions that wouldn’t be possible without identity. In other words, identity lends predictability to afford a comfortable level of confidence for people making decisions.
4. **Identity is referential.** An identity is not a person; it is only a reference to a person. Even if a person develops spin-off personas so that other people know him through those various digital identities, and even if others create profiles of a person, ultimately the collection of characteristics that signal who a person is need to point back to that person.
5. **Identity is composite.** Some information about a person arises from the person himself; he volunteers it. But other information about him is developed by others without his involvement.
6. **Identity is consequential.** Because identity tells of a person’s past actions, the decision to exchange identity information carries consequences: Disclosure of identity information in a certain context can cause harm; failure to disclose identity information in another context can create risk.
7. **Identity is dynamic.** Identity information is always changing; any particular identity dossier might be inaccurate at any given moment.
8. **Identity is contextual.** People have different identities that they may wish to keep entirely separate. Information can be harmful in the wrong context, or it can simply be irrelevant. Keeping identities separate allows a person to have more autonomy.
9. **Identity is equivocal.** The process of identification is inherently error-prone.

* *The Properties of Identity were articulated by Bob Blakley, Jeff Broberg, Anthony Nadalin, Dale Olds, Mary Ruddy, Mary Rundle, and Paul Trevithick.*

Content in this text box is licensed under a Creative Commons Attribution 3.0 License.

Does an Identity Framework Need to Be *Global*?

Does identity management introduce new problems or opportunities that are global in nature and that require a coordinated, international set of rules or guidelines? Participants identified certain challenges that seemed to point to the need for global cooperation in policy and law concerning aspects of identity management. Some participants saw potential to support a global identity infrastructure, while others saw significant risk in that approach or felt that many challenges could be addressed more locally.

Openness in the Identity Infrastructure

A number of participants argued that the construction of a system of identity systems, or an infrastructure, should be a goal of global policy, and that a vital dimension of this was to have international policy and law promote an open infrastructure.

In order for identity management systems to serve people effectively, different systems need to be able to work together, and to tie into an overall infrastructure spanning the globe. If countries pursue systems that interoperate, they gain the advantage of being able to connect for shared goals – for example to encourage e-commerce, facilitate international travel, counteract cybercrime, advance global health, and thwart the financing of terrorists, among other aspirations.

Beyond having systems that work together, it will be important for an infrastructure to be sufficiently flexible to accommodate new entrants to the market and new technological approaches. Competition policy on a global scale could be well targeted to these aspects of an identity infrastructure, for example to prevent concentration in the market for service providers and to prevent vested interests from blocking out new offerings. Competition policy could also thwart collusion among parties that handle personal data.

Accountability of Persons and Governments

The ability to be recognized as a person digitally is increasingly necessary for an individual's basic participation in society. More and more, people will need digital identities not just for transactional convenience, but in order to be perceived by others as having existence. Few actions will take place without authentication and authorization playing a part: It is likely that digital identities will increasingly be required for banking, transportation, communications, building entry, and other everyday facets of life. As such, people will be dependent on an identity infrastructure.

The trend is for governments to provide citizens with digital identities in order to facilitate official interactions with government online as well as private transactions online that require accountability. That said, some participants cautioned against being too ambitious in developing a forward-thinking global plan: A plan with fine-grained detail would likely prove futile when it came to global implementation.

Still, a few participants contended that a global framework is needed for registry services that can help authenticate people and lend others assurance that the parties with whom they are acting are legitimate. The idea is that such assurance would empower people to interact globally. Such registry services would seem to require technological interoperability and legal harmonization (following a common approach) or at least mutual recognition (different jurisdictions reciprocally accepting each others' approaches). Although the idea of a centrally administered system of globally unique identifiers was raised, other participants contended that a more practical and politically acceptable approach would be for governments each to operate registry services in a similar way as they run the passport system: With the passport system, every state has its own chosen format that is within the internationally agreed standards and procedures for cross-border travel documents. In other words, although a global framework might need to cover registry services, it need not entail a single "world roll"; rather, a global framework could facilitate coordination among states, each of which could run its own roll.

Points relating to these issues are relayed in the sections that follow.

How Should a Global Framework Respect *Local Values*?

The workshop discussion took a surprising turn when considering how a global policy and legal framework for an identity infrastructure should accommodate local values.

Starting Assumption that Respect for Local Values Is Proper

The implicit starting assumption for the discussion was that local values should be respected. After all, while it may be true that an identity infrastructure needed the support of a global policy and legal framework, it still the case that people around the world have different values and do not want a global system to work against them.

Thus the question was originally posed as: “How might a global framework accommodate local values?”

Questioning Whether Respecting Local Values Is Always Desirable

However, the discourse revealed that this question overlooked the more fundamental issue of whether such local accommodation was always desirable.

Say that an identity infrastructure could be used to effect “zoning”, where claims indicating location and/or citizenship would be used to determine which jurisdiction’s laws should be superimposed to give a “local” setting for a person’s activities.

An example of how this zoning could operate in practice, and how such an arrangement could be designed to account for local values as reflected in law, is the case of data protection (putting aside for a moment the issue identified above that for data protection to work in practice, a global approach is needed). If Region 1 has rigorous data protection requirements and wants to allow its citizens to engage in commerce with Region 2, which normally allows entities to do what they wish with data they can collect, there needs to be a way to signal that the data of the party from Region 1 must be accorded strong protection. If entities in Region 2 do not want to transact with parties from Region 1, they can choose to deal with parties from elsewhere.

Another example of how zoning might be applied to protect local values is in the area of freedom of expression: Country X favors minimal constraints on freedom of expression, while Country Y holds this right dear but at the same time tempers it in light of the need to ensure that the right is not used to perpetrate hate crimes. If the identity infrastructure were equipped to handle zoning, then a blogpost by someone in Country X that advocated neo-Nazism could automatically be filtered so that viewers in Country Y would be spared from seeing it.

A tension arises when the ability of an individual to choose is introduced. It appears that the international legal arrangement is such that people can choose to have less autonomy – for example, a particular jurisdiction might have strong data protection standards but permit citizens to consent to transactions with service providers elsewhere that treat identity information with less care; but people have difficulty choosing greater autonomy – for example, a person living in a jurisdiction where the government will not allow her to build up a credit line due to her gender, ethnicity, or faith would have greater autonomy if she could access services offered by, say, MasterCard or Visa. Should the international system recognize her right to act outside the confines of her home jurisdiction? Would such an approach support universal human rights (in this case, the right to own property, without distinction of any kind, such as sex, race, religion, or jurisdictional status), or would it advantage some actors over others?

Despite freedoms spelled out in the Universal Declaration of Human Rights, the international legal system in practice tends not to “interfere” with certain government policies toward their citizens. For example, international market access commitments typically allow a regime to make exceptions for matters of public safety, privacy, health, or morals. Countries may have bound themselves to observe certain freedoms by signing the International Covenant on Civil and Political Rights, but in actuality there is little enforcement by the governments of signatory countries.

Given how integrated the world could be through online systems, this potential zoning through computer code appears to conflict with the notion of universal human rights. Human rights advocates ask whether it makes sense for the international system to condone the use of computer code to fence in citizens. For people living in places where the law does not accord them basic human rights, a global framework designed to respect local law in essence is reinforcing injustice. Should the human rights that a person enjoys in the information society depend on where he or she happens to be born in the physical world? Perhaps in the future there will be some sort of competition among governments to attract digital citizens, and this competition could serve as good incentive for governments to treat digital rights more seriously.

Global and Local

Global and local are not necessarily incompatible alternatives. A good deal may depend on the types of information flows in question. Flows within one jurisdiction – say, between Edinburgh and Oxford – could require one kind of solution, while flows between different jurisdictions – say, from Oxford to India – would require another solution. To avoid a tangle of bilateral arrangements, some level of alignment of approaches, through mutual recognition or even harmonization, would be needed. This alignment could entail an international or supranational system with predictable rules for how to cater for various discrepancies and differences.

This prospect leads to the question of whether country membership or commitment to an overarching legal framework would be necessary for exchanges. A federation in the legal sense could be one approach, but there would need to be a centralized forum where members could decide principles for when rules would be determined locally or globally. This arrangement would be analogous to the United Kingdom (UK) with respect to the European Union, where the UK must adopt certain laws at the national level to align with European Directives. The UK would not necessarily adopt some laws if there were not some sort of higher-level governance structures. In the case of identity management frameworks, a federal model (in the legal sense) might provide a mix between global and local regimes.

Would domestic governments grant such powers to a higher, federal body at the international level? Over time might the direction shift, so that the local would find itself needing to comply with policy and law decided at the federal level? Coordination among peer entities in a federation could lead to the centralization of functions as the membership sets up institutions over time to allow members to better coordinate activities and policies on a more regular basis; these institutions are likely to accumulate expertise and eventually assume decision-making power. In such ways, coordination to align countries’ policies for identity management can be understood to have potentially wider implications than just facilitating information exchanges – which is one reason why some jurisdictions are likely to resist such approaches.

Minimalist Approach

Bearing in mind stakeholder demands for predictability, as well as the serious implications that would flow from establishing a global framework, a more conservative approach would be: (i) to limit ambitions for global approaches to the minimum needs, (ii) to treat issues at the plurilateral level (involving several countries) or even at the bilateral level if international coordination is necessary but can be avoided at the global/multilateral level, and (iii) where possible to decide issues at the domestic level. In other words, the principle of subsidiarity should apply, with policy and law set at the most local level that is feasible.

Where international coordination appears necessary, countries could choose to exclude “rogue states”. This approach could favor an identity infrastructure that was in line with liberal democratic values. This approach would permit the establishment of identity frameworks at the plurilateral level in advance of a time when the conditions existed to establish global processes. In other words, it could be better to give attention to the minimum arrangements needed at the global level rather than to strive for an ideal global system that might not be approachable at this time. Once a basic structure was in place, other systems could be built on top of this structure.

Is a Framework *Feasible*? How Might It Be *Achieved*?

In considering whether a framework is feasible and, if so, how it might be achieved, workshop participants talked about encouraging a family of systems through policy and law. Attention then focused on the need to promote trust through competition and through transparency and accountability. In addition, the group considered how best to spur the development of a policy and legal framework (even if minimal), including the need to raise public awareness at an appropriate stage.

Family of Systems

Different Systems Using a Shared Infrastructure

There are different types of identity management systems for different uses. For example, one type of identity management is privilege and entitlement management, where organizations are sharing data about people. This type is sometimes referred to as a top-down, organization- or government-centric system. When doing transactions, the organizations want to make sure that the data really pertains to the person in question, even as the person interacts on a global scale. To do this type of identity management globally, from any point A to any point B, requires some form of unique identifier for every person. These types of systems require very strong security measures and give rise to numerous questions about privacy, autonomy, misuse, and so forth. Another type of identity management involves self-asserted identity data, sometimes referred to as user-driven or user-powered. Here a person can just port his or her identity information across all kinds of places all over the world; the challenges there are completely different, with much less security demanded.

Participants considered whether there were a core set of features that could lead to a family of systems that could all be part of the same infrastructure. In terms of a business model, both identity providers that would attest to claims, as well as service providers that would rely on them, needed to be able to establish themselves to make money. For a thriving ecology, users should have choices when they dealt with providers of various kinds.

Risks in Borrowing Approaches Designed for Different Uses

Experts discussed the implications of borrowing an identity management system that was designed for a simple type of use and applying it for other types of uses. For example, if a government used popular, simple federation technologies without security, there could be dire consequences in terms of loss of autonomy and security. Some participants predicted this borrowing would occur as governments sought to roll out user friendly systems on a broad scale by building on systems that were already popular and had wide acceptance.

Identity management as a business is fairly sophisticated, but it is also high risk. Those entities that at first glance would seem to be the natural constituencies for engaging in identity management as a business are mature and therefore may actually prefer to avoid risk so as not to expose the businesses they have built up over time. The people interested in green-field opportunities may be more like the “webkiddies” from San Francisco, who have nothing to lose and see no problem jumping into spaces that are highly risky if an opportunity presents itself; they are especially keen if risk is tilted away from them and toward users.

Different Models

One participant described the central government in a typical country as a single organization; with information sharing among governments, the many national governments across different countries may then be thought of as effectively parts of the same single organization. In that sense, the individual has a relationship with that government monolith, which may extend across many different countries. The drivers for that kind of identity management today are anti-terrorism, anti-fraud, security generally, money laundering, etc. This kind of coordination and use of identity management systems is likely to continue gradually as technology becomes cheaper, as the needs become more pertinent, and as the governments become more capable.

Meanwhile, to grow user-centric identity management systems proved difficult, and in essence posed a true infrastructure problem. Individuals may intensely feel the need for such systems, but large organizations do in only very small degrees. The people who have the funds and the ability to start large projects tend to be those within large organizations, who start these projects for the purposes of their own organizations only, as the profit motive would dictate. They are motivated to do what is good for the individual only when there is a clear business case. It would be unrealistic to expect private businesses altruistically to look after the public interest. It would seem society needs an infrastructure in which individuals are empowered to choose the terms of treatment for their identity information and to see that they are enforced; such a system must also be accessible and affordable.

Although some experts contend that a user-centric system would be a public good and would require public funding, others see a business model emerging for this approach. As discussed at the workshop and noted in the issue brief by Iain Henderson (appearing in Annex III): Mydex will equip an individual to say: “‘My view of me’ is vastly superior to any other view of me; where proof is required I can bring that proof; my view of me looks forward, organisational views of me look backward. Give me the necessary tools, incentives and protections, and I will share that view with organisations which respect the terms and conditions I set around that access.” Hence the tables are turned as the individual (or “data subject” to whom the identity information pertains) is both the user AND the data processer/handler.

Reliable Access and Concentration in the Market

Because the Internet is global, people will expect an identity infrastructure also to work on a global level. Identity management should not depend on the Internet service provider (ISP) or the country where a person is logging on – rather, a person should be able to have all the services delivered no matter where he or she logs on from. There is this expectation of reliable access wherever a person will be. Can that be achieved?

Longer term, de facto economic power should also be considered. It is conceivable that there could be a lack of competition, resulting in concentration in the market, with just one or a few identity providers dominating the worldwide market. With that market power, they would be able to dictate the systems that society uses. Competition policy could address this, but, again, it might need to apply at the global level.

Swedish Lessons in Openness

A lack of interoperability in design specifications could dampen the utility of any given system. An example in point is the BankID model in Sweden. In contemplating options, the government reached the point where it said, "We do not want as a government to create an identity management service; rather, we want to buy one or rent one." They therefore wrote the specification for identity management, and periodically they would go out to the market and ask who wanted to provide the service. Among other contenders, most of the banks got together and created a little company called BankID. It became the dominant provider. It entailed a very strong PKI based system. The banks already had experience in knowing who their customer was and in doing secure online banking; the government said they would rent these services. It was a simple model: Literally, the banks guaranteed a person's identity through the enrollment process, and then they rolled out a strong PKI based service so that when that identity was presented, it was quite believable. This identity is what an individual would present to government when that person wanted to do business with government.

At first glance it would seem that the Swedish system should be scalable internationally, as banks are everywhere. For two key reasons the Swedish example illustrates that sometimes the local approaches are not scalable to the international level: First, there is a lack of a global competition-policy regime (which could require, e.g., technological interoperability). Second, costs of using the system may be prohibitive for some key uses.

These are international dimensions of the limitations experienced domestically with the program in Sweden, but the constraints arguably can be addressed by factoring in a wider set of objectives at the outset. In negotiating the contract, the banks had sought technically to strap a very limited identity management business on top of the banking business; meanwhile, the government decision-makers were anticipating that citizens would use the system for tax filings, in which case the fee for certifications seemed reasonable. Additional successes could have been achieved if the technical system had been designed with interoperability in mind and with the contract reflecting this (allowing other developers to set up gateways with different interfaces), and if the fee structure had factored in everyday usage (making frequent usage affordable, so that, e.g., students could use the system for physical access to university buildings). Through the process early lessons were learnt; adaptations have been made, leading to a reasonably successful situation, but it is likely that more will need to be done.

Roots, Accountability, and Geo-Politics

Accountability through Linkages

As already evidenced today, a person will likely have multiple digital identities for use in different contexts, for example professional or social. Some experts say that for activities requiring an official identity, a person's various digital identities could refer to a "root". Each person could have one official root, from which he or she could generate identities for use in various contexts. By linking identities to the root, enforcement agencies could track people down to hold them accountable for actions. Linkages could facilitate other aspects of public safety, health, national security, etc. as governments would have an easier time correlating data. If this were the desired scheme, governments would need to cooperate to ensure that each person had one and only one root identity. Coordinated registry services could appear the logical approach. It was suggested in discussion that areas of namespaces in the Internet's domain name system could be assigned to governments, which could then distribute unique identifiers to their citizens.

On the flip side, it is possible that a root or unique identifier would be used to link a person's data into a super account, which would be a honey pot for attackers as well as governments and other parties seeking to implement concepts and programs that many would consider inconsistent with human rights or basic concepts of dignity. So, too, an insider with access to the data could impersonate a person and do great damage. Beyond individual cases, there would be widespread destruction if the mapping system suffered a successful attack.

Indeed, a system of globally unique identifiers could encounter problems regarding public trust in government. Some fear that unique identifiers would bring a chilling effect as citizens felt subject to extensive surveillance or, worse yet, that the identifiers would in fact usher in extensive surveillance. People could find themselves dependent on an international registry service for transactions requiring use of a root. Indeed, they might even be required to use their root for very access to the Internet. In other words, authorities running the unique identifier system would be in a position of great power. If there were an international registry service housed in a non-local institution, it is unclear how this power would be directly accountable to the public. With potential power to grant or deny a person the ability to transact in the information society, it is within the realm of imagination that such a service could even determine who counted as people.

Multi-party security can ensure global accountability even when a user's actions are unlinkable and untraceable; it is possible to "ban" a user from multiple services where he or she uses unlinkable identifiers, on the basis of misuse of any one of these services, through the magical "blacklist revocation" technique. In this respect, it is important to note that (1) the ability to have accountability by being able to "ban" users is not the same as being able to trace those users, (2) the blacklist revocation technique does not involve a "key escrow" agency that can trace and link if it wants to, (3) the escrow agency feature is a separate feature, which may be relevant if traceability should be necessary without any involvement of the user, and (4) for certain "bad" actions it is possible to achieve such traceability if and only if an untraceable user "misbehaves."

Mitigating Some Contamination Risks

The process behind root issuance would arguably be a weak point in terms of trustworthiness as some countries would be digitally corrupt, with government departments looking to commit fraud. In response to this criticism, the hierarchy of the namespace system would allow segmentation to allow questioning of roots issued in places of dubious reliability. The system would incent countries that wanted to participate as full participants in the global economy to align or harmonize their procedures for proofing, registration and enrollment, and for the subsequent provisioning of attributes or claims, so that citizen identities issued by them or certified entities in their jurisdictions would be accepted as meeting standards for higher levels of assurance. The plurilateral approach would be a reasonable way to have a critical mass of countries align their approaches in other ways as well, for example to spell out compliance requirements, liability, and so forth.

Some experts see unique identifiers with namespaces as offering a good solution for enabling identification of citizens for official interactions with government and for achieving accountability for private dealings that tie to such identities. It has been suggested that, because the structure of the namespace system has a hierarchy, it would allow segmentation to prevent roots of low assurance levels from bringing down the trustworthiness of the system. This approach would help screen out roots issued by countries where corruption in the identity system is known to exist.

Marginalization of Least Developed Countries

However, beyond flagging identity claims that might have been issued in a corrupt process, this segmentation by assurance levels would also screen out identity claims issued by countries that simply do not have the resources to implement a secure system nationwide. In at least 60 countries, a major challenge is registration of births and deaths. They lack the technical infrastructure, the know-how, the human resources, and the finances to support it. In other words, there will be marginalization of some countries and their populations. These countries are likely to be the same ones that already suffer from marginalization in economic terms – i.e. the least developed countries. If these countries are cut off from the identity infrastructure, they will have even greater difficulty participating in the global trading system. Their people's already harsh conditions will likely deteriorate if action is not taken to include them in the identity infrastructure.

Therefore, when considering what is feasible for a global system and how different systems might work together, it is important to factor in these constraints and to look for ways to address them.

Countries' Differing Priorities and Capacities

Not all countries have identity management as a priority right now. Nevertheless, exigencies of security make those countries that do care want to extend an identity infrastructure to whole world. Trade interests should make all countries care since regions that use interoperable systems will likely experience greater economic activity.

Fundamentally, conditions are not the same everywhere in the world. It is important not to lump all countries together but instead to distinguish their needs and interests.

Rich countries are characterized by high income and established economies. There are about a billion people living in such countries. Infrastructure is quite good, and there is continuous improvement. Costs are stable, and there is advanced research and development. There are many incentives for applications development. (For example, applications in the health space are proliferating.) These countries already have legal and regulatory systems in place. They have a very large and pro-active middle class using ICT, and that population is driving expectations. There is much new pressure: not just from consumers, but from associations and academics. In terms of what is hindering improvements in areas like eHealth, there are political compromises and industry interests that are antagonistic sometimes. In short, there are a lot of stakeholders, and they are not aligned.

In emerging economies, the picture is somewhat different: These are middle income countries, and they have high growth rates. There is a very strong political will to match the living standards of the rich countries, and technology is seen as the key to obtaining this goal. Generally there is (a) increasing public demand for services, (b) lots of investment in infrastructure, and (c) an emergence of local industries and services. Mobile is established and broadband is coming. The key in these countries is that they want to be like the rest of the developed world. Hence, the industries and the governments are very motivated to adopt standards, regulation, and legislation that can harmonize with others and that can improve their economies. Still, financial and human resources are rather limited. That factor will impact on the ability actually to implement identity management systems. Governance, transparency, and public trust are highly variable and not a given, and the incentives and policies are still at early stages. Countries are starting to adopt, almost wholesale, legislation from other countries that might not be appropriate to their own environments.

Then there are low income countries. They have gross domestic product (GDP) per capita of US$1000 or less. Today there are 70 countries in the lowest income group, and another 44 just above that. They face very significant challenges politically and have fragile health systems and limited infrastructure of all types. There are many pilot projects, and scaling up is rare, so there is no single, systemic picture. They have emergent public demand. Mobile telephony is experiencing high growth. These countries are most prone to disasters and conflict. Infrastructure investment is mainly donor supported and very low in terms of resources across the board. The people are desperate for policy change.

Internet Governance and Geopolitics

Dr. Viv Padayatchi contends that the Internet is well positioned to become “the underlying medium of choice” for supporting the identity infrastructure. “The identity infrastructure will make use of several application layers of the Internet Protocol (IP) network.” Examples include URLs, the world wide web, routing protocols, name resolution, and encryption. Padayatchi explains (see Annex III):

> At the heart of the Internet infrastructure management are the global namespaces such as “com”, “net”, “org”, etc. They are known as the global top level domains or gTLDs. The country namespaces (“uk”, “fr”, “de”, etc.) were added later and are referred to as ccTLDs or Country Code Top Level Domains. In parallel to the namespaces is the number space which refers to the pool of IP addresses (e.g., 196.3.111.20), which is allocated to operators around the world. The mapping of the name space to the number space and vice-versa is the basis of the Domain Name System or DNS. Today, all aspects of the management of the DNS ultimately links to the umbrella organization known as ICANN (Internet Corporation for Assigned Names and Numbers)…

The DNS is not without its discontents on the world stage. A key aspect of DNS geopolitics is “the association of ICANN with the US Department ofCommerce (DoC). Through this association, ICANN is viewed as being, ultimately, accountable to the US Government.”

During the workshop it was noted that these geopolitics can be expected to come into play in global policy debates on using namespaces as the means by which governments would issue unique identifiers to citizens, and in debates on other Internet-related issues of identity management.

Promoting Trust through Competition, Transparency and Accountability

Obtaining society's trust will be fundamental to the success of any identity infrastructure. How do policy and law support trustworthiness in the identity infrastructure so that the public's trust is justified?

In considering different models, questions to consider include: Are there certain aspects of the top-down, government-federation model or the bottom-up, user-centric model that are more trustworthy? If an infrastructure enables both models to be used, should policy and law require the use of identities issued from the top-down authority for official dealings with government and for private interactions that require accountability? Or would it be better for policy and law to take a flexible approach so as to leave greater room for innovation? Whatever avenues are chosen, it would seem important to keep all control points in the infrastructure open to competition so that different systems can compete and new technologies can be added.

Risk Shifting

One participant maintained that, ever since Reagan and Thatcher, there has been a very broad social trend of shifting risk away from organizations. The whole of the Internet is being built on a gradual risk shift away from organizations and onto individuals. Perhaps at the start this shift was right, but arguably it has gone too far the other way. Now it is strikingly similar to the economic externalities in the environmental system: I pollute, you pay. In this instance, it is like the recent financial crisis: "I can take the risk, but you pay for it."

It would seem that young people especially have borne the brunt of this risk shifting. How can a policy and legal framework address people of all ages (with changing needs as they grow) including the lost generation whose data has already been released?

What should a policy and legal framework say about identity management systems that attract users due to user friendliness, but that leave these users vulnerable to phishing? Is it acceptable for companies offering services in such systems to avoid liability if users consent to the arrangement?

Structural Safeguards

To discourage corruption, the system structure should be architected to pit interests against each other through checks and balances, and to keep functions distinct with a view toward separation of powers, particularly among chokepoints in the infrastructure. So, for example, a single government should not have monopoly power over the issuance and certification of root identities. In certain parts of the world, redress for mistakes in issuance will not be possible. So rather than having local authorities issuing identities, perhaps domains of authorities would be more appropriate, where there would be several authorities or institutions that could issue claims about different aspects of someone's status. That way a person would not be subject to just one entity without an opportunity for appeal. The idea is to build some safeguards into the system.

An international, interdisciplinary team could be commissioned to design into policy, law, and technology an assortment of mechanisms that shore up freedoms and rights, especially those that are essential for correcting problems. Specifically, these freedoms include privacy, expression, and association/assembly; and in terms of rights, a key one is access to information in a timely manner, even when private entities are carrying out governmental functions.

In the interest of privacy and security, policy and law should favour a technical architecture that enables “minimal disclosure”, whereby the minimum amount of information necessary for a transaction is transmitted. Linking of information from different transactions should not occur unless a user specifically wants these correlations. The structure of the system arguably should prevent the linking of identifiers.

Of course, governments will sometimes assert the need to collect and use people’s personal data without their knowledge. To maintain public confidence, policy and law could call for the infrastructure to build in oversight by independent ombudsmen whenever such instances occur, so as to ensure that any such activity is always legal and that governments are not overstepping their prescribed powers.

There should be transparency in the technical structure and also in policy and law. There needs to be auditability of all information flows through a record of all actions taken at points along the path of any given information exchange. When systems span jurisdictions, transparency and accountability throughout the chain of information exchange are particularly important. There need to be global standards for auditing.

Even with these precautions, policy and law for an identity infrastructure need to encourage technology design that has suspicion built into the workings. What was scary about the role-play scenario with the wrongdoers was that the system could be described to others in such a way that it appeared to be completely benign: There were standards, there was a mechanism for governance, and there was auditability. None of those statements were incompatible with the fact that the system had a completely subversive goal. Separating powers could help because it would increase the number of functions that a subverting party would have to undermine; if these powers were pitted against each other (e.g., had competing interests), they would be more likely to check to see that nobody was trying to gain control over the infrastructure.

Currently, none of the systems that are being designed build safeguards and recourse in as fundamental requirements. All of the systems are built on an optimistic basis.

User-Friendliness Now and Eventual Imperceptible Workings

At this early stage it is important for identity management systems to be user friendly and to have a consistent user experience to help people adjust to it. Arguably there is a security interest in this consistency since people are more prone to being taken advantage of by bad actors when they are presented with varying ways of doing things online. In terms of uptake, the more that identity management actions are a barrier between people and what they want to do, the more hostile they are toward systems. How do designers make the user experience engaging or smooth, or make systems actually help people?

In the future ambient intelligence environment, where all these kinds of solutions will run in the background, people will no longer see them. The solutions will be automatically implemented and should run in the background. While this background quality will spare users from having to deal with details, a policy and legal framework should be crafted to ensure that fair information principles work even in that setting so that, for example, people are aware when they are passively releasing data about themselves and have a way to require others to treat it according to their conditions.

Encouraging the Uptake of Privacy Enhancing Technologies

There may be rules and stipulations as to what can and cannot be done in different contexts. Binding policy to data could be a way to enforce these obligations through technical means.

The trouble is that technologists know how to bind policy to data (with tags and audit trails, etc.), but nobody is showing demand for these solutions to be developed.

Similarly, it is possible through cryptography for an identity management framework to facilitate the building and maintenance of reputation(s) while respecting privacy. However, for technology developers to invest heavily in designing such systems, they need to know there is customer demand for the solutions.

Policy and law can be crafted to affect the designs of software providers, similar to the way that carbon emission limits constrain car engine manufacturers.

"S-curves" crystallized the idea that there are roughly twenty different factors that can play a role in speeding up the adoption of privacy enhancing technologies. (See issue brief by John Borking in Annex III.) By knowing what these factors are, policy strategists can try to focus on them and devote policy and legal attention to them to speed the incorporation of privacy enhancing technologies into the ecosystem.

Anticipating Failure

For consumer protection today, it is important to set up light-weight regulators like information commissioners because they are able to do something for the citizen at almost no cost to the citizen.

One could imagine that a governance body might be established to clamp down on inappropriate practices and help people obtain redress.

Breach notification laws could have an effect on the service providers, making them want to store less data and to treat it with great care. Here again, transparency and accountability, as well as good competition, can go far in creating the right incentives.

In Europe, the Service Directive creates a drive towards reporting about activities in e-services along the chain. Yes, it entails more legislation and more rules. But it is still a viable question whether the information society should have similar types of rules in the area of data handling rules as it has for money handling. This is not to say that the money handling rules are good, but rather to recognize that data handling is becoming as important as money handling.

Security experts say it is extremely important to be able to attribute failure. For example, failures at the network layer can harm a business' reputation. It might not be clear where the failure is – it could be a failure at the level of the domain name system, or at the level of routing, or elsewhere. Entities responsible for different functions in the infrastructure are at risk from the layers beneath that might not be trustworthy.

In Europe there has been discussion about changing consumer protection law at the European level. The software companies have been successful in keeping liability for failure out of their ambit for the time being. To some extent this dodging is reasonable, as the software companies are looking to see how best to share liabilities in their internal relationships in the chain. But before long the politicians will likely be forced by consumers to place responsibility on the software providers. Cloud computing adds a huge multiplier in the degree of difficulty of chasing down these chains.

For cases where the blame for failure lies with government, it is difficult to hold anyone responsible. An example of a lack of redress for citizens may be seen in the infamous HMRC data loss in the UK. This case involved a failure of process in the public sector, with its roots in poor risk assessment and all those contributing factors. As a result of the data loss, people will be suffering harm over time, with significant negative consequences expected to manifest themselves in a few years. People may claim that the harm stemmed from that instance of data loss, but their chances of proving it will be nil. In the wake of that event, one workshop participant talked with policymakers about ways in which data breaches could be made more auditable or traceable, such that data found in the wild after a breach like that could be more reliably traced back to the person or entity responsible. The officials were not the slightest bit interested in features that could lead a trail back to them. There is strong incentive for government not to put that kind of auditability in place. Absent building in such auditability, it will be almost impossible for anyone to attribute the subsequent damage to that event, especially when there are international dimensions.

With respect to liability and trans-border data flows, many APEC members are of the view that Europe's approach to enforcing data protection law internationally has not worked. A company in Australia had been arranging for direct marketing phone calls to be made out of India back into Australia in a way that violated Australia's "do not call" policy. For enforcement the regulator had a choice of going after the local Australian company or chasing the companies in India. The regulator went after that Australian company as doing so was cheaper and had a multiplier effect. Essentially the idea is that the company remains accountable for whatever it causes to happen through the rest of the value chain. That entity is thereby forced to internalize the costs of the risk and to figure out how to share these costs with others it contracts with throughout the chain. The effect is to place on that entity the costs of enforcement, freeing the regulator from having to spend its resources chasing down those in other jurisdictions. Criteria for assessing a measure might thus be: Can you make it span jurisdictions? Is it cheap and effective? Does it send the right signals?

Cloud computing presents enormous difficulties for current law. A study came out this year saying that much of what is done now in company clouds is illegal, but nobody is aware of it. A simple example: If a company moves data from the United States to Europe, and then moves that same data to India, from the moment it is in Europe onward, European law applies, and the Safe Harbor provisions should be applied to the move to India. The parties often are not honoring the law, and the data is flowing around regardless. Current law is not able to deal with these trends. Some fundamental rethinking is needed rather than just some adaptations of the law.

To pursue a remedy at all, one must be able to know how data has been treated. Policymakers could encourage the development of global audit standards, and law makers could add pressure, for example by enacting legislation requiring that technologies in the identity infrastructure support fair information practices (e.g., by enabling end to end auditing).

Spurring the Development of a Policy and Legal Framework

Assuming it was clear what should be the substance of a policy and legal framework to support an identity infrastructure, there would still be the issue of agreeing to such a framework through the policymaking process. Strategic questions include: Who has to be influenced? What is being asked of them? What are the various levers and buttons for convincing them? When does the message really get heard and acted upon? And what are the actions most likely to lead up to that point?

At some stage there will be a tipping point when the need for this framework becomes a "Tier 1" issue for global leaders, but much time could pass before then. People eager to take action in the meantime could try to achieve objectives organically. Many groups might be interested in participating in this organic process, including technical standards bodies (e.g., the W3C and OASIS), trade associations, and non-profit organizations. This organic process could at the very least help raise awareness among leaders and articulate alternatives for their consideration.

Model Laws, Standards, and Principles

Establishing a global, regulatory regime all at once does not appear to be an option. Again, identity management is serving different purposes in different places at different stages of development in different systems in countries. Even though different countries are taking different approaches, at a certain point they come to the same problems discussed here. Those who were further along could offer a solution that others could draw from to factor in the lessons learned – a sort of "open regulatory framework" (like open software): They would be free to take and use it if they liked.

Such approaches are not new to the international policymaking community. Model laws are often promulgated, for example by organizations like the United Nations Commission on International Trade Law, which has crafted such recommendations as the Model Law on Electronic Signatures and the Model Law on Electronic Commerce.

In countries that do not have regulation and legislation, standards play an incredibly important role, be those standards from industry or from another particular community. If those standards were crafted well, they could be in place for a long time before regulation would be necessary. Standards can therefore be very instrumental for the global picture.

Similarly, more generalized principles could go far in providing guidance. A set of principles would not be a stringent approach, but rather would allow flexibility.

Building Blocks in Local Approaches

In light of the need for certain worldwide approaches on the one hand, and the challenges of reaching agreement and then implementing it on the other, the objectives of a framework might best be achieved by starting at the local level. Through a voluntary federation process, local approaches can grow and in time establish a model for a global approach. This is the method that appears to be underway in reality.

A feasible approach would be to encourage the embracing of general principles at the multilateral or plurilateral level (e.g., in the OECD), and then to see if this set of principles could spur thinking for implementing systems and ideas at the local level. The actual activity would be at the local level, where the different locales could learn from each other. There could be benchmarking, trials, and so on, with the local levels helping each other set rules.

General principles agreed at the global level could include a principle that the local governments should avoid putting into place laws or regulations that act as barriers to different systems' working together. If there were such principles, they could also indicate a desire for increased integration in the future, so as to signal to local interests that they should expect a certain direction over time, and that local measures would be subject to realignment if that jurisdiction were to participate in that larger integrative effort. More specifically, the principles could call on local regimes to build into legislation and regulation a review process for reexamination of the rules. The plan would be to draw on experiences of different places to see which approaches were most successful; the different local regimes could then build coalitions and agreements to come to a more regional or global approach.

The European Union itself is an example of this gradual, integrative process.

For policy prescriptions, it is not just a matter of having the right thing to say, it's a matter of saying it at the right time so that it falls on receptive ears. In emerging economies, it may be the case that the only form of regulation that is needed is to set a standard, and to wait until later to follow that up with legislative measures. It may be that a rather general global "governance framework" is appropriate, an that under that governance framework, at different points in time depending on the maturity of the audience, various measures could be introduced in the form legislation, standards, best practices, and self regulation. A policy and legal framework is a good objective, but as an early step perhaps countries need something expressed in general terms so as to allow flexibility in terms of which societies should apply what measures in which contexts at what time.

This formula describes the Asia Pacific Economic Cooperation (APEC) process of coming up with a governance system for transborder data flows. The regional grouping uses a relatively loose definition in order to afford members leeway to set specific rules in accordance with their own assessments.

Toolbox of Policy and Legal Measures

Drawing from regulatory theory, "carrots and sticks" could be an effective means of incenting the right kind of behaviors to lead to a balanced ecology. For example, the prospect of commercial gain could serve as a carrot, and the threat of penalties for non-compliance could serve as a stick. To compare various options for carrots and sticks available at different levels of government, policymakers could use a matrix, with carrots and sticks on one axis and global-regional-national on the other. Policymakers could then analyze the pros and cons of different regulatory instruments and strategies at different levels, and consider what kinds of actions could be taken to promote them.

Certain drivers could serve as sticks: For example, regulations might need to address transparency and require reporting on the use of data.

Intergovernmental Cooperation on a Sectoral Basis

It is possible to leverage sectoral initiatives to support the creation of a policy and legal framework.

Health is considered a public good and thus is an area where international policymakers engage. At the local level, some countries have systemic health problems, including enormous problems with surveillance of infectious diseases, provision of care over long distances, rural health worker shortages, and international problems with drug and supply chain management. Health systems in poor countries are not integrated. At the same time, there is a good deal of international cooperation in the health sector: A community of biomedical researchers actively collaborate from all around the world; specialists in infectious diseases carry out coordinated international surveillance; and countries have signed onto treaties that commit them to follow common policies to promote public health. These are the sorts of things that could be very important in identity management, especially as health is a driver for ICT infrastructure.

The World Health Organization (WHO) represents this particular sector and, as an international organization, has its own set of interests according to its mandate. WHO could press for global definitions of liability with respect to health data in identity management, and the organization could also raise awareness of the limits of identity management with respect to health (whereas other sectors, e.g., education, may have their own interests and may see other limits).Perhaps most importantly, WHO could play a direct role in assisting developing countries to craft identity management policy as it pertains to global health.

Of course, a sectoral approach would presumably need to proceed in parallel with other efforts that would factor in the multiplicity of stakeholder interests.

Awareness Raising

Questions on the political side of policymaking include: Who is setting the agenda – the individual, organizations or government? Who has the most to gain from this? What governmental and political buttons need to be pushed to develop a framework? What do they understand about any of this, who should be their audible and disinterested teachers, and what action should they take?

To inform the policymaking process, it would be good for there to be an expert body, or expert bodies, to provide input. These experts could operate at local and global levels, and they could also provide advice on sectoral approaches that span both. Such expertise could help others understand the implications that different measures might have on the workings of an identity infrastructure. With their citizens' interests in mind, governments could avoid much grief if they would seek such input before taking action.

Because there can be de facto regulation of identity management as a consequence of policymaking in other areas, it is important to engage with specialists on those other issues. For example, there are topics currently debated, such as cyber security and child protection, where the dialogue is focused on regulation as a way to solve a problem, without an idea as to how to implement it. A dialogue about identity management could usefully inform those other issues.

Participants considered the Internet Governance Forum (IGF) as a process that brings together businesses, governments, and civil society from all over the world, convening in one place for four days to discuss emerging governance issues relating to the Internet and its use. The IGF does not have a mandate to make decisions or recommendations, but it is a talk shop where stakeholders come together to discuss issues. At its heart, the IGF arguably is a forum about government responsibility to engage in debate on broad policy issues. For many governments thinking at a high level, the IGF is the forum where there is debate about things like who controls the Internet. The importance of identity management may not yet be grasped, but workshops could help bring attention to it.

(It was noted that some people feel that simply by virtue of participating in the IGF, one is contributing to the institutionalization of a sort of global governance for the Internet and the way the Internet is used; and that given the blurring of the distinction between the real and virtual worlds going forward, this basically suggests global governance. So some people fear participating in this forum because they think they would be inadvertently furthering the cause of global governance.)

There are many existing forums where there are ongoing dialogues. Rather than saying, "We must all converge in one particular place," some would prefer to ask, "How do the different corners each have effective conversations with the constituencies they are dealing with?" and then "How do we bridge these different conversations?" Many discussions are taking place concurrently, and the groups are not doing a good job of collecting their outcomes in real time and connecting the people who wish to be engaged. The communities working on this topic could all do more to share information. Identity Commons is an example of one association that formed to coordinate among groups. The structure places nobody in charge, and a high value is placed on sharing information to build trust and collaboration amongst the many groups.

Whereas one view held that talking about policy and law before the technical infrastructure emerged would be premature, a different view held that it takes time to line up cooperation in policy and law. While this technical and policy and legal evolution is happening regionally, and federations form and lead to a more global approach, it would make sense to begin an international, multi-stakeholder discussion in anticipation of the longer term. Put more strongly, before the world’s people would be subject to a global or even regional or local regime, should they not receive information and have a voice in the process? Waiting until the system is up and running would seem to limit the public’s choices.

For wider public outreach, people who are already well informed about the issues should find ways to communicate ideas. They should try to use media like cartoons, YouTube videos, and diagrams to teach some of the core ideas that experts have refined over the years. It would be appropriate to engage with people leading civil dialogue processes within countries and to dialogue with citizens to generate public conversation in a way that would help good outcomes to result.

The social implications of this technology are immense. It would be best to leave no forum that deals with related issues devoid of discussion about a policy and legal framework for an identity infrastructure. One must participate if one is to influence the agenda. Experts who are heavily involved in this discussion should be careful not to take it for granted that everybody is aware of these issues to the same extent. It is highly important that this kind of informative discussion take place in any arena that’s talking about new ICTs and their application. One needs to be a fish out of water occasionally to realize how vital it is to be involved in these forums.

ANNEX I: Data Protection at Service Points in the Identity Infrastructure

The current vision for an identity infrastructure raises a number of issues for policy and law to clarify regarding data protection. To consider these issues, it is useful first to review basic components of a possible identity infrastructure.[4] Here we assume that components include:

- The parties involved in exchanges;
- Agents through which the parties request and pass information; and
- Personal data, as contained in "claims".

Here is an example of an interaction involving the different components:

The user employs a computer agent (e.g., a web browser or software program) to request services from a service provider (sometimes called a relying party).

1. In response, the service provider informs the user's agent, through a technical policy statement, what personal data, or claims, it requires about the user.

2. The user's agent presents these requirements to the user through a "claims selector". If the user decides based on this information to consent to the transfer of the required personal data, he instructs the claims selector to contact a "claims provider" that stores his personal data for him.

3. As the claims selector contacts the claims provider, it presents proof that it is operating on behalf of the user. (This proof may be a sort of key, sometimes called a "primordial claim", that will have been established previously through a "registration" process.) Then the claims selector conveys the service provider's technical policy statement to the claims provider.

4. The claims provider uses its own technical policy to determine what claims it should issue in response (e.g., claims with minimal disclosure). The claims provider then initiates "claims transformation" and issues the resulting claims to the claims selector.

5. The claims selector forwards the claims to the service provider.

6. Once the service provider receives the requested claims about the subject, its "claims approver" assesses whether the claims are reliable (e.g., whether they have arrived intact, if their origin appears legitimate, if they are fresh, etc.). The service provider will employ its "resource matcher" to associate the claims with information that the service provider already has about the user (e.g., account information). The service provider will then provide personalized service.

This document serves as a first cut at analyzing some of the data protection issues that arise with "service points" of the envisioned identity infrastructure. This analysis may prove helpful in identifying issues that a public policy and legal framework should address in order to create a predictable environment for the information society.

[4] These components are elaborated in "Proposal for a Common Identity Framework: A User-Centric Identity Metasystem" by Kim Cameron, Reinhard Posche, and Kai Rannenberg (2009).

Claims Selector

This service point raises the following questions, among others:

Should there be a legal obligation for this service and the relying party's agent to speak the same language and communicate to indicate Purpose, Use Limitation, etc.? If so, should there be a standard format (syntax, schema, etc.)? Should this be machine-readable, human readable, and lawyer readable? If not, is notice of practices effective?

Primordial Claim

This service point raises the following questions, among others:

If presentation is cross-border, it could entail a release of personal data in a manner that is contrary to a jurisdiction's law. Do legal systems with such requirements imply that primordial claims should go through a local anonymizer that can issue a derived claim for (primordial claim key-like) access to the identity provider? Would such requirements necessitate a legal sanctioning or official recognition of geolocational services and/or zoning to signal an individual's location or citizenship?

Registration

This service point raises the following questions, among others:

Who is authorized to do in-person proofing? If a private sector entity is, do obligations apply as if that entity were a state actor? (If so, is the entity still held to standards for private actors as well? How is this determined? Does it vary by jurisdiction? If it varies, what are the implications for a framework?) Does the need to prevent duplicate registration necessitate a central registry service? If so, how is such agency governed?

Claims Provider

This service point raises the following questions, among others:

Do individuals have the right to decide technical policy, or is this something that public policy will leave to the market to determine? Either way, should public policy/the law promote or recognize a standardization of options, for example along the lines of icons to reflect data protection preferences/choices – and should public policy/law encourage a correspondence of these options to expressions of relying parties' technical policies? Should public policy promote the development of the ability of individuals to signal (anonymously) preferences for how their data is treated so that they may act as a group and not have to negotiate individually against a large entity? Should economists advise on this public policy? (Since it seems this collectivity would discourage price discrimination and restore consumer surplus, etc.)

Claims Transformation

This service point raises the following questions, among others:

Are there certain cases for which minimal disclosure should be mandated (e.g., for voting)?

Claims Approver

This service point raises the following questions, among others:

Should public policy/law require this service point, the Claims Selector service point, and Claims Provider service point, to speak the same language so as to enable communication and negotiation of policies? When receiving data and assessing it to decide whether it meets requirements in advance of providing services, should a relying party take on some obligations with respect to what is disclosed at that stage, even if it then decides based on the claims received not to provide the anticipated service – and how might a contract reflect this separate obligation?

Resource Matcher

This service point raises the following questions, among others:

Should the relying party be required to indicate, in advance of receiving claims, how those claims will be matched with data it already has, and how this resulting profile will then be used? Should the data subject have access to the information that the relying party has on file and whatever assessment has been made of that data? Should the data subject have a right to know in advance to whom that data may subsequently be passed? *Etc.*

Service Points as a Group

This service point raises the following questions, among others:

Should there be auditing requirements for all service points? If so, should these requirements be standardized? How? Where?

ANNEX II: Comparison of Models for Transferring Identity Information

From The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers, OECD, DSTI/ICCP/REG(2008)10/FINAL

	Siloed	**Centralised**	**Federated**	**User-Centric**
Method of Authentication	The user authenticates to each account when he wishes to use it.	The user authenticates to one main account.	The user authenticates to an identity provider, with this one authentication serving for the federation.	The user authenticates to identity providers, and service providers have to rely on that authentication.
Location of Identity Information	Identity information is stored in separate service provider accounts.	Identity information is stored in the one main account, a super account.	Service providers in the federation keep separate accounts in different locations. They may have agreements for sharing information.	Identity information is stored by identity providers chosen by the user, who can help prevent the build-up of profiles that others hold about him.
Method of linking accounts/ learning if they belong to the same person	There is no linking between accounts and no information flow between them.	Linking between accounts is not applicable. (A user's full profile resides in that single place.)	The identity provider can indicate what identifiers for accounts with federation members correspond to the same person.	Uses of cryptography can prevent linkages between a user's different digital identities, leaving the user in control.
Trust Characteristics (who is dependent on whom, for what)	The user is reliant on the service provider to protect their information, even if limited. The absence of information sharing has privacy advantages.	The user is reliant on the service provider to maintain the privacy and security of all of his data.	Users have rights from contracts, but they may be unfamiliar with options. The federation has leverage as it is in possession of the user's information.	Users can keep accounts separate and still allow information to flow... [If he uses multi-party security, the user gains privacy, and the service provider gains security against user fraud.]
Convenience	Siloed accounts are inconvenient for users and service providers due to multiple authentications, redundant entry of information, and lack of data flow.	This arrangement is easy for the user since he or she only has to deal with one credential to call up the account and since he or she has to authenticate just once.	Other members of the federation avoid the burden of credential management. Organisations that provide services to a user can coordinate service delivery.	Users may be ill-equipped to manage their own data (also a vulnerability) and may need training and awareness-raising.
Vulnerabilities	Siloed systems offer the advantage of having limited data on hand, thus creating less of an incentive for attack. They also have a better defined and stronger security boundary to keep attackers out and limit exposure from failures.	The central party controls the person's entire profile; other entities have little to check that profile against, and an insider could impersonate the person or alter data. Currently there is no way to safeguard data after it has been shared.	Users have little input into the business-partner agreements. Some service providers will set up federation systems to exploit users. Currently there is no way to safeguard data after it has been shared.	Concentration in the market for identity providers could leave them with much power. Currently there is no way to safeguard data after it has been shared.

ANNEX III: Issue Briefs

John Borking:[5] Maturity Model for Privacy and Identity Management (PIM)6

To examine under what conditions an organization would adopt PIM into its business processes, we have to examine the privacy management (PM) and identity & access management adoption (IAM) maturity in organizations. The hypothesis behind the choice for the IAM maturity model[7] is that as protection of personal data is closely linked with identity issues, the increased attention for identity in the organizational processes must lead to the awareness of informational privacy.

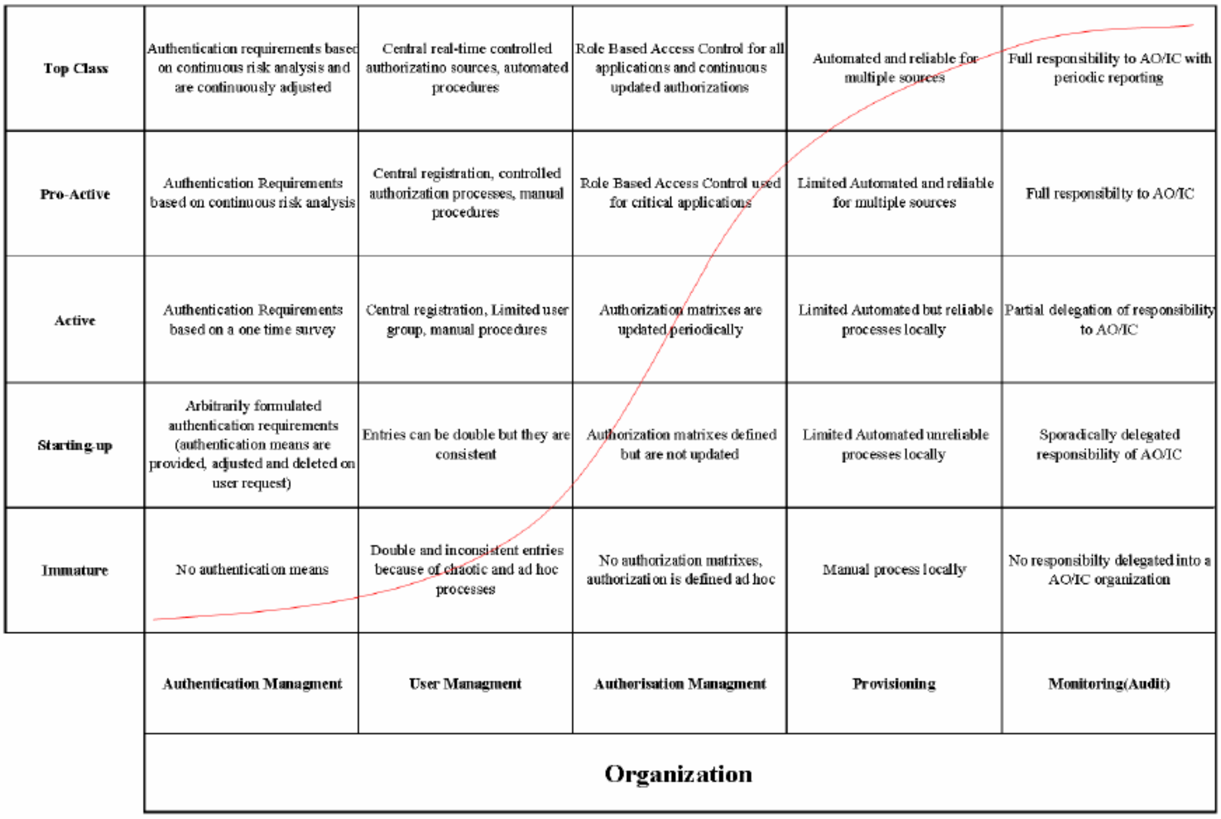
[5] John Borking is owner/director of Borking Consultancy in Wassenaar The Netherlands and former board member of the Ditch Data Protection authority

[6] Identity Management without privacy management will become privacy intrusive

[7] A maturity model is defined as “a staged structure of maturity levels, which defines the extent to which a specific process is defined, managed, measured, controlled and/or effective, assuming the organization develops and adopts new processes and practices, from which it learns, optimizes and moves on to the next level, until the desired level is reached.”

Maturity Model

During the last decade several maturity models have been developed in specific research areas such as business IT alignment, software development and information security. All of these models have one thing in common; they all describe the maturity of one or more processes within an organization. Every model characterizes the first maturity phase as being chaotic and dealing with processes on an ad hoc basis. The second maturity level is characterized by the planning of processes. The third maturity level is characterized by the implementation of standards aimed at particular processes and outputs for processes are defined. Quantitative management characterizes the fourth maturity level. Processes and quality are controlled based on quantitative measures. Based on the measures taken out of the quantitative measures implemented in maturity level four, maturity level five improves the organization. These improvements are continuous, incremental and connected to the business objective measures. Through all of these five maturity phases the awareness and importance of IAM processes increases within the organization. The organization going through all these sequential phases not only needs to adjust its identity and access management processes, but also its own organizational structure and policies need to be adjusted. These adjustments like the adjustments to the IAM processes need to be evolutionary not revolutionary.



Top Class	Authentication requirements based on continuous risk analysis and are continuously adjusted	Central real-time controlled authorizatino sources, automated procedures	Role Based Access Control for all applications and continuous updated authorizations	Automated and reliable for multiple sources	Full responsibility to AO/IC with periodic reporting
Pro-Active	Authentication Requirements based on continuous risk analysis	Central registration, controlled authorization processes, manual procedures	Role Based Access Control used for critical applications	Limited Automated and reliable for multiple sources	Full responsibilty to AO/IC
Active	Authentication Requirements based on a one time survey	Central registration, Limited user group, manual procedures	Authorization matrixes are updated periodically	Limited Automated but reliable processes locally	Partial delegation of responsibility to AO/IC
Starting-up	Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and deleted on user request)	Entries can be double but they are consistent	Authorization matrixes defined but are not updated	Limited Automated unreliable processes locally	Sporadically delegated responsibility of AO/IC
Immature	No authentication means	Double and inconsistent entries because of chaotic and ad hoc processes	No authorization matrixes, authorization is defined ad hoc	Manual process locally	No responsibilty delegated into a AO/IC organization
	Authentication Managment	**User Managment**	**Authorisation Managment**	**Provisioning**	**Monitoring(Audit)**
	Organization				

Figure 1 IAM maturity model with S- growth curve

If the rights to access can be bound to a certain group, profile, person or user within an organization then IAM can be used to make sure that the user or user group only gets access to the information for which they are authorized. IAM then can also be used to provide the means of identification to make sure that the right user gets access to the user profile that is authorized to access certain sensitive information. Next to user management, authentication management and authorization management, provisioning and monitoring and audit can also play an important part in awareness for privacy management and PETs (privacy enhancing technologies) implementation.

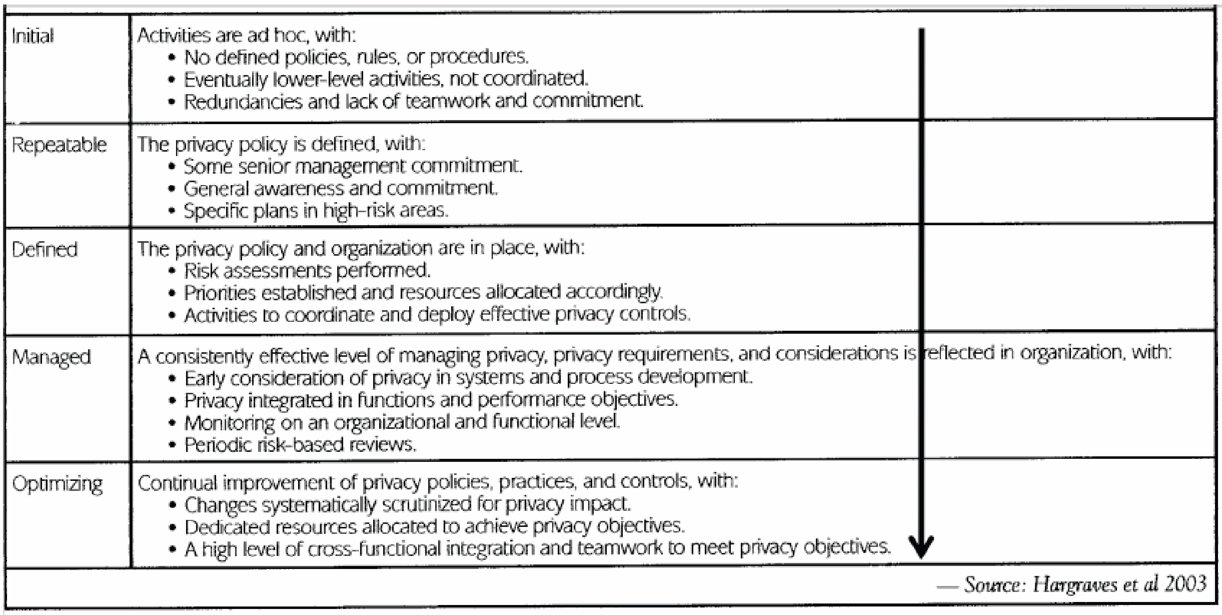
For the implementation of privacy management and PETs, a certain maturity of the organization is required. It is highly unlikely that immature organizations will have any awareness of privacy management and will implement PETs. Research[8]showed that the level of maturity for IAM is a strong indicator for the introduction of privacy management and subsequently PETs in an organization.

Based on this model it is predicted that privacy protection and PETs will be applied by organizations at the maturity level "Active" and upwards. There are exemptions for those organizations that belong to the category of (micro/mini) SMEs where trust is a critical success factor, like in the medical profession, barristers, notaries etc. Although the processes mentioned in the maturity model are non-existent, it may be expected that those SMEs will protect personal information of their clients encrypted or will use rudimentary PETs tools.

Three S-Curves

The IAM processes follow a S-Curve. The same can be concluded for privacy protection. In an interview for a case study concerning PETs investment the CPO of a Dutch multinational said that "To align the different interests within our organization you have to look at the privacy maturity levels. For comparison we use the standard of the GAP Institute of Internal Auditors (GAP schema GTAG 5). "The GAP privacy level scheme follows a S-curve as well".

The GAP GTAG 5 scheme is as follows:



Initial	Activities are ad hoc, with: • No defined policies, rules, or procedures. • Eventually lower-level activities, not coordinated. • Redundancies and lack of teamwork and commitment.	
Repeatable	The privacy policy is defined, with: • Some senior management commitment. • General awareness and commitment. • Specific plans in high-risk areas.	
Defined	The privacy policy and organization are in place, with: • Risk assessments performed. • Priorities established and resources allocated accordingly. • Activities to coordinate and deploy effective privacy controls.	
Managed	A consistently effective level of managing privacy, privacy requirements, and considerations is reflected in organization, with: • Early consideration of privacy in systems and process development. • Privacy integrated in functions and performance objectives. • Monitoring on an organizational and functional level. • Periodic risk-based reviews.	
Optimizing	Continual improvement of privacy policies, practices, and controls, with: • Changes systematically scrutinized for privacy impact. • Dedicated resources allocated to achieve privacy objectives. • A high level of cross-functional integration and teamwork to meet privacy objectives.	

— *Source: Hargraves et al 2003*

Figure 2 Processes in the development of privacy protection

For PETs solutions the S-curve is also applicable. The combination of the three S-curves leads to the figure 3 indicating a model of decision-making for IAM, PET and Privacy management.

[8] P. M.A. Ribbers, PRIME (Privacy and Identity Management for Europe, EU research project Contract No. 507591(2004-2008), Privacy Process Requirements, Brussels 2007

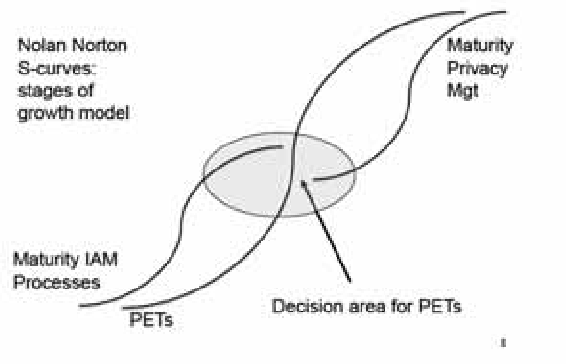


Figure 3: S- curves for IAM, PET Privacy Mgt

Christopher Brown

Introduction

Access and Identity Management (AIM) is a key component of many initiatives across JISC and as such the Innovation Group works closely with the Services and Collections Teams. This work involves both the support and expansion of the UK Access Management Federation as well as looking at how new developments can both improve on this service and how innovation might help increase the uptake of access to resources and information within the community. Previous programmes in AIM have focused primarily on the technologies used to provide good access and identity management, with a gradual shift towards exploring the issues around policy and process. The AIM programme[9] now aims to focus on process, policy and technology, exploring innovative new areas in all three and forming a natural complement to work being completed under the Services banner on the UK federation.

With the move towards user-centric identity where individuals can control what identity information is released the assertion of identity becomes an increasingly important issue and requires that the relevant legal framework for user validation is in place. This issue brief will focus on the policy and legal issues raised by the **assertion of identity** as well as some of the areas that are affected by this assertion. It does not attempt to resolve these issues but rather to invite responses as to how they can be solved. It should be stressed that a user-centric approach is not a threat to the Identity Provider method used for the Federation. There is a need for both so in the future a mixed economy is likely to result.

User-centric Identity

Current access to resources, especially within the UK Federation, is very much tied to an individual's institute. The institute provides the identity to the individual and the federation allows access to the resources that have signed up to the federation. However, with increasing numbers of lifelong learners and new learners seeking retraining there are potential users who are either not tied to one institute, or are part of an organisation that is not part of the federation. When a person leaves one institution and joins another, the transferring of identifiers between these institutions raises certain issues that require legal and policy frameworks to be in place.

For example, an institute, or in fact any organisation, may require paper copies of certificates before a person can start a new job. How can the details of an individual's qualifications be

[9] http://www.jisc.ac.uk/whatwedo/programmes/aim.aspx

taken with them to other institutions, once they leave that institution, in the same way as paper certificates? This could all be done electronically if a user's details / attributesare stored with the user's credentials and taken with the user and trusted by the organisation. However, this would require one institution to **trust** the credentials and attributes from another institute or trust these details from the individual.

The user-centric approach, in which the assertions are made by the individual, would require the relevant legal framework for **user validation**, providing user access to information that might be shared by other institutions. When an institution makes available a personal identifier that might have been used by an individual at previous institutions, they are asserting things about that individual's previous history. Or conversely, they are making assertions about future uses of the identifier. This will require the institution to trust or vet an individual's previous employers. If this assertion proves to be false the institution may be legally liable. The solution to this problem would be to have this controlled by a named authority service.

When a person leaves an institute the user's identity is **de-provisioned** and a new identity created when an individual joins another institute. A user-centric approach, where the institute effectively hands over the user's details, would enable the lifespan of a user's identity to extend beyond the lifetime of their work within an institute. Their work record would be preserved and transferred, for example certificates, passing units, research records, attendance records, etc. Storing some of these attributes has legal implications especially in the area of **data protection and privacy**, especially if some of these details were used by the new institute to the detriment of the individual. There is also the issue of **ownership** of this information. What is owned by the individual and what is owned by the institution? The technologies are there to implement these features but we must ensure that the policies and legal framework are in place to protect both the individual and the institution.

Levels of Assurance

Both the Registration and Authentication types of Levels of Assurance have policy and legal implications. Identity registration is establishing a relationship between a user and an identity provider. This identity must be verified to establish that the user has the right to assert that identity. At registration it is important to ensure that the relevant checks are made and the user is given the relevant level of assurance. This process needs to be formalised and agreed across institutions for it to work. With authentication, however you are authenticating yourself, whether it be username and password, PKI certificate, etc the level of authorisation must be set correctly.

OpenID

OpenID, which is increasingly being used in social networking communities, may also be applicable in Higher Education and research environments. There are problems with the levels of assurance provided by an OpenID. However, it may be interesting to disaggregate the use of OpenID to identify oneself from the authentication/assurance aspects; the OpenID could then be used as an attribute within the federation, but with federation methods used to provide the trust. Alternatively, one could use OpenIDs supplied only by providers that conform to additional conditions, although this may break the benefits of OpenID. OpenIDs could be enhanced by "white lists" where an institute trusts the providers of the users' credentials. What is clear is that we cannot overlook the user experience and user authorisation and authentication should be as seamless to the user as possible.

Granularity

Access to resources via the UK Federation currently has an all or nothing approach. This lack of granularity of access is a problem for certain organisations especially ones that give access to sensitive data. Where views of the data need to be restricted to particular individuals using roles or groups this not only adds to the complexity for the administrators of the resource, but the relevant policy of the institute must be complied with. Of course there are the legal issues involved in ensuring the data is protected. Increasingly an audit trail of updates, views and queries on the data is required. The controlled access to these resources requires a strong form of identity assertion.

Conclusion

In this brief the assertion of identity has been explored and how it affects a number of areas in identity management. As more institutions require access to an increasing number of resources and as individuals increasingly demand a more user-centric approach as they become increasingly mobile, the policy and legal frameworks that enable this to happen must be in place. The JISC Innovation Group will be looking to fund more of the technologies that support these developments but will ensure that the importance of having the relevant legal and policy frameworks in place is not overlooked.

Jaques Bus and Dirk van Roy: Informal note on privacy & identity in the digital society & economy in response to the guiding questions of the draft agenda[10]

This note is written from the authors' perspectives of their work in the area of trust and security in DG Information Society and Media at the European Commission, but it does not represent official viewpoints. For the sake of completeness, the mission of DG INFSO is to stimulate the development of the information society in Europe and to increase competitiveness, growth and employment. The three main instruments used are: 1/ regulation and policy, among others for providing a level playing field; 2/ support to RTD through the ICT Research Programme, part of the 7th RTD Framework Programme; and 3/ stimulation of uptake and use of ICT, in cooperation with Member States.

Trust and security are horizontal issues cutting across many different domains of the digital society and/or the ICT Research Programme. These include the areas of eHealth, transport, eGovernment, eInclusion, eCommerce, eBanking, social networks, forums, virtual environments, eNews, and others.

Trust - the overriding concern

With the rapid proliferation and development of the information society trust and security have increasingly been recognized as pivotal elements for the continued growth of digital life, society and economy. The single overriding concern and pre-condition for digital interactions and transactions is the presence of a sufficient level of trust, either explicitly and consciously acknowledged or implicitly taken for granted (rightly or wrongly, without further thought). Trust is a relational property and not a measurable system property. It is elusive, subjective and depends on context and culture.

A whole body of literature and analyses is available on issues such as security, trust, privacy, identity, data management, accountability, transparency etc. For the current purpose, it suffices to say that in the digital world the level of trust depends on many

[10] *The views expressed in this note are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.*

variables, including the ability to sense the trustworthiness of third parties, to assess recommendations and reputations, the availability of a legal framework and the ability to exercise the rule of law, the scope for redress and trustworthy conflict resolution, the ability to be in control of releasing data and to audit their use, to undo the release of data and so forth, but also the dependability and resilience of the technology, systems and networks used, the security features of the systems and services, compliance seals etc. Some aspects can be easily "rated", measured, assessed or verified; others cannot. In short, trust depends on a wide spectrum of intuitive and non-intuitive indicators, subjective perceptions, more or less agreed societal conventions, a multitude of legal systems, properties of the digital systems themselves and the degree of user control and verification.

To complicate matters further, the digital society transcends geographic, jurisdictional and cultural borders, and ICT systems are composed of heterogeneous technologies, networks, services and policies. There is no steady-state baseline or anchor point; to the contrary, the digital society is subject to an unseen rate of change and metamorphosis of services, applications and paradigms. Against this background, it may look like an impossible task to forge trust and dignity into the digital society. And yet, in the authors' view, as it has been reasonably mastered in physical life, adequate set-ups should be possible and this should be part of the objectives of our work. Despite all the threats on the Internet, humans seem to have an unstoppable desire to participate in digital life and a knack for finding ways and means to avoid, limit or mitigate the worst pitfalls. Yet, for all we know, we are at a very early stage of the digital evolution, and bearing in mind the historic experiences of societal developments, we need to carefully consider the options available and find a balance of where we usefully sh/could interfere to preserve a free and open society, avoiding getting trapped in surveillance or profiling (governmental or commercial), and avoiding mind-numbing measures or restrain creativity, while providing trustworthy fabric for digital life.

A changing world – the role of technology and law

The rule of law, in particular civil law,[11] received a strong impetus with the introduction of book printing and gained effectiveness onwards. The prevailing mindset became characterized by reflective and sequential processing of information. It is worthwhile noting that law enforcement is primarily based on detection after the facts, and there is a notion of 'relative relevance', i.e. are enforcement, detection and providing proof worth the costs?

The advent of the Internet, with random and instantaneous access to all kinds of information by a simple click, has re-tuned human information processing with parallel and ad-hoc processing elements. One can speculate if the 'contraction of space and time' in human information processing in cyberworld might affect the traditional sort of protection that law can provide. Or, that at some stage, in principle, systems could be set up to easily detect 'all' illegal actions of some sort, so that there is no cost/benefit issue of substance. The changes brought by new ways of interacting in cyberspace may very well be the beginning of a recalibration of the role of regulatory instruments in society. The Commission in its first report on the implementation of the Data Protection Directive considered that "…the use of appropriate technological measures is an essential complement to legal means and should be an integral part in any efforts to achieve a sufficient level of privacy protection…" [COM(2003) 265].

The role of identity and identity management

Identification is crucial in life, and 'proper' identity management is a crucial element of a European trust approach in digital life, society and economy. The ability to prove claimed

[11] The debate of common law versus civil law is beyond the scope of this note.

credentials that are proportional to a context, and not to be continually monitored, watched and registered, is fundamental to the preservation of a free and democratic society.

For historic reasons identification is weakly defined in the current digital world; there is a lack of an identity framework and an identity management infrastructure. This has led to paradoxical uses of identity information. Sometimes identification is so strong and wide, often not by conscious choice or intention (for example based on habits such as checking a passport without registering its data, but only to control that the person is who s/he claims to be), to the extent that it unduly enters the private sphere if all data would be registered and used for yet undefined or undisclosed purposes; in other situations mutual identification is much too weak for the purpose at hand (for example in situations that need strong and *specific* identification of parties entering a transaction). Both types of situations are problematic and undermine trust-building, provide room for abuse, and ultimately might have a negative impact on the continued development of the information society.

The problem is that there is no well-developed vehicle for electronic identity management (though several initiatives and approaches have been proposed by various parties, leading to lack of integration and interoperability). A proper eIDM mechanism is needed to ensure trustworthy identification, adapted to the requirements of a given situation and under the control of the person who owns the ID credentials. Multi-facetted IDs that can be released under the users' control, the absence of unintended linking capabilities, and proper protection of the ID data are some of the elements for trustworthy eIDM.

An eIDM infrastructure is needed for trustworthy interactions between public authorities, businesses and citizens, and for trustworthy services in domains such as e-government, e-health, e-commerce, finances, web 2.0 communities and the forthcoming internet of things. It needs to be anchored on a wide (EU, global) privacy-protective eID approach going across all domains of the digital society. It should support the provisioning of multiple identity instances from government-accredited to commercially accepted, and ranging from near-anonymity to strong identification. This should start from a user-controlled and privacy-protective perspective and provide the basis for accountability and innovative applications in an open and competitive service market.

David Chadwick: No Position, But Trying to Establish the Correct One

One of the dilemmas that is currently being faced in TAS3 is how to balance potential legal requirements, such as the recently suggested idea of Facebook, Flickr et al. keeping an audit of the links that are generated between users (or their virtual identities), with the technical possibility of the AAA infrastructure hiding real identity information from applications, and inhibiting different service providers from colluding to link together the different virtual identities of a user. Should the AAA infrastructure actively try to prevent applications from determining who (in terms of physical entities) are involved when virtual identities are used and linked together, or should the AAA infrastructure try to ensure that "real" identity information is given to applications so that they can know who is behind the virtual identities. The virtual world must touch the physical world at some point e.g. when a credit card is used for an online purchase, when a user contracts with an ISP for a service, when an IP address is given to a PC. So it is very hard to be 100% virtual with no physical linkage at all (even when using an Internet Café you have to physically go there). The issue is how hard should the AAA infrastructure make it for service providers (or others) to be able to either bind a physical identity to a virtual one, or link the different virtual identities of a user together. Should the AAA infrastructure make it as difficult as possible for law enforcement (and others) to bind virtual identities to physical ones.

It is hoped that this workshop will shed light in this area and indicate where the optimum balance should be, so that the technical infrastructure can be built to support this (but no more).

Piotr Cofta: Trust assurance: a foundation of identity management

1. We consider here regulatory aspects of the adoption of a citizen identity management system ('identity card system') from the perspective of trust relationships within sociotechnical communication systems.

2. There are certain perceived social benefits of a citizen identification system, yet countries differ in realising them, usually in accord to the extent of trust in institutions (operators) that administer such scheme (Backhouse and Halperin, 2007).

3. Adoption of technical systems is not driven by trust in technologies, but by trust in the operators of such systems. Assurances regarding such a trust, in the form of regulatory framework that supports restitution measures and demonstrates duty of care are essential (Lacohee et al., 2008).

4. Individuals are aware that no security system is perfect and that over time, any identification system will eventually be compromised. Promises regarding 'unbreakable' security decrease trust in the competence of an operator (ditto).

5. While individual rejection of a citizen identification system is not essential to the success of the system, wider rejection amongst the population may deprive the system (and the operator) of all its benefits, leaving it only with burdens.

6. Legal, technical and procedural choices that an operator can make are not semantically neutral, but they are interpreted as a message from an operator and affect the relationship between the operator and individuals (Cofta and Lacohee, 2009).

7. For a citizen identity management system, the asymmetrically dominant role of a government as an operator of such a system calls for very through consideration regarding the message of trust (ditto).

8. One of key functions of an identity management system is to communicate and reinforce (thus assure) trust in goodwill intentions of the operator of such a system. Note that an alternative trust assurance perspective (that seeks the operator's assurance of trust in the identity of an individual) is not considered here.

9. Currently in the UK the government is not seen as 'connected' and is not trusted with individual's data. However, individual government agencies can be trusted to some extent (Lacohée and Phippen, 2007).

10. The key message that can instil and reinforce trust is one of privacy protection because privacy is valued by the majority of individuals (Lacohée et al., 2008).

11. Privacy is understood here as contextual integrity, where the use of personally identifiable information agrees with regulatory legal and implicit social expectations (Nissenbaum, 2004).

12. There is a relationship between privacy and trust; the need for trust increases the desire for privacy and anonymity but the existence of trust decreases it. It is beneficial for all

parties to address the need for privacy through trust rather than through anonymity (Cofta, 2008).

13. Any legal, technical or procedural choice should be tested against four scenarios, as follows (Cofta, 2009):

    1. Benevolent state. This scenario assumes the goodwill of 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.

    2. Pragmatic state. This scenario assumes that the state's continuous struggle to maintain the identification system gradually erodes the idealistic approach of the benevolent state and shifts it towards a more realistic one where data is being shared with businesses for commercial gain. The most important feature of the system is therefore to minimise function and information creep.

    3. Incompetent state. This scenario assumes that the state intends to operate the identification system, potentially in a pragmatic way, but due to its incompetence allows data to be stolen, misplaced, altered or otherwise abused. 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.

    4. Malicious state. The final scenario assumes that the state has installed an identification system and that over time, the operator of such a system has become malicious. 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.

14. Further, there is a strong need for continuous dialogue because inherent social creativity will eventually embrace and re-purpose the system, in a process where individuals will express their perception of their identities (Giddens, 1991).

References

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

Cofta, P. (2007). Trust, Complexity and Control: Confidence in a Convergent World. John Wiley and Sons.

Cofta, P. (2008). Confidence-compensating privacy protection. Proc. of PST2008 Sixth Annual Conference on Privacy, Security and Trust.

Cofta, P. (2009) Towards a better citizen identification system. Accepted for FIDIS Journal.

Cofta, P., Lacohee, H. (2009) Trust in identification systems: from empirical observations to design guidelines. Accepted for publication in Trust Modelling and management in Digital Environments: From Social Concepts to System Development (Eds. Dr. Zheng Yan).

Giddens, A. (1991). Modernity and Self-identity: Self and Society in the Late Modern Age. Polity Press.

Lacohee, H., & Phippen, A. (2007). Trust and Government in the UK - A Grassroot Perspective. Paper presented at the Trust Conference, The Hague, Netherlands, November 21-22 2007.

Lacohee, H., Cofta, P., Phippen, A., and Furnell, S. (2008). Understanding Public Perceptions: Trust and Engagement in ICT Mediated Services. International Engineering Consortium.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. Washington Law Review, 17, 101-139, 2004. Retrieved June 10, 2006 from http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf

Malcolm Crompton: User Centric, Layered, and Global: What sort of Policy and Legal Framework?

Introduction

There are a number of privacy and trust challenges for managing identity on the internet. The policy and legal issues are complex and frameworks to handle them are only slowly evolving. Governments and other organisations are finding that addressing domestic issues only solves half the problem. This is because managing e-identity is rapidly becoming a global as well as a domestic issue. Whether domestic or global there is clear evidence that one of the keys to unravelling a number of the conundrums is the need for a stronger focus on the user in developing frameworks.

The great risk shift

Users are starting to realise that when an organisation moves its service to the online environment, the organisation often manage their own risks by shifting the risks on to the individual. In the context of identity management solutions, this “great risk shift” often means:

- Stringent requirements are placed on individuals to identify themselves, but no attention is paid to assuring the individual that the organisation is who it says it is (ie no provision for mutual trust);
- Little attention is paid to the security and secondary use risks from the greater ease of aggregating data about an individual through the use of unique identifiers;
- Little attention is also paid to the consequences of the huge volume of peripheral data that could be collected through the digital footprint every time individuals electronically identify themselves;
- The inconvenience for individuals (or worse) if the system fails or when individuals loses their means of identifying themselves.

Current approaches fall short

A number of attempts to adopt identity management solutions have also run into trouble with the community because they have not been sensitive to the impact that identity management initiatives may have on the ability of users to exercise control over their lives and their identities. This is often blamed on an undue focus on the technology of the proffered solution and only from the point of view of addressing the needs of the organisation. Regulation of e-identity has tended to focus on compliance with existing (and rapidly becoming outdated) law, or only on changing existing laws so that current impediments can be circumvented.

Part of the answer does lie in technology and in the law but there are also some other, more nuanced strategies that must come into play to create the trust in new identity management solutions.

User Centric Identity Management one key

There is an increasing body of thinking around what has become known as the ‘user centric’ approach to identity management. Early work includes reports from the London School of Economics (LSE) in response to the UK Identity Card proposals, Microsoft’s Kim Cameron’s ‘Laws of Identity’ and the work Information Integrity Solutions.[12] More recently, we have seen commercial investment in such solutions, including the purchase by Microsoft of the U-Prove technology[13] and the inclusion of the Idemix technology in the Higgins Open Source Identity Framework.[14] The European Commission and its research partners in the academic & commercial sectors are also investing significantly in user centric ID management including in the PRIME & PrimeLife projects.[15]

Our analysis suggests that organisations must consider three dynamic factors from the point of view of the individual to encourage mutual trust. These are:

- **Fair risk allocation** – ensuring that individuals understand the risks and are confident that they are fairly allocated to the party most able to bear them;
- **Control** – ensuring that individuals have the control they want over how information is demanded, collected and stored, or if that is not possible or wanted, they understand the organisation and are confident that it will handle the information appropriately;
- **Accountability** – ensuring that the organisation is accountable and transparent about how it will handle personal information and take appropriate responsibility for dealing with the impact of failure on the individual including having a good safety net.

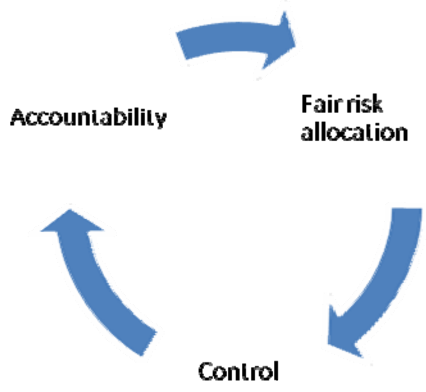
These factors are dynamic and interdependent. All components must be addressed from the user’s point of view to achieve trust, but some may need more emphasis depending on the circumstances. For example, where people perceive a high level of personal risk, they may demand increased personal control. On the other hand, where an organisation displays high levels of accountability, including transparency, individuals may perceive that there is less risk, and may demand less levels of direct personal control.

[12] “The Identity Project, An assessment of the UK Identity Cards Bill and its implications”, Chapter 18, ‘Design Principles and Options’, London School of Economics, June 2005 (http://is2.lse.ac.uk/idcard/; “The Laws of Identity”, Kim Cameron, May 2005 (http://msdn2.microsoft.com/en-us/library/ms996456.aspx); “Proof of ID required? Getting Identity Management Right”, Privacy Commissioner Malcolm Crompton, March 2004 (www.privacy.gov.au/news/speeches/sp1_04p.html); “Trustguide”, a Sciencewise programme funded by the Office of Science and Technology in the UK Department of Trade and Industry, October 2006 (www.trustguide.org.uk).

[13]See www.microsoft-watch.com/content/security/microsoft_says_u-prove_it.html and www.identityblog.com/?p=934

[14] See http://wiki.eclipse.org/Idemix_Provider.

[15] See www.PRIME-project.eu and www.PrimeLife.eu respectively



How these dynamics play out may depend on the legal, historical, cultural environment, including whether the organisation is public or private sector and the purpose for which identity management is being implemented.[16]

Layered defence strategies needed

Instead of relying only on technology, or on a very narrow, one size fits all use of law, it would seem more advisable to apply a 'layered defence' approach that draws upon a combination of the following tools as necessary and appropriate to achieve both the goals of the project and the privacy needs of individuals and society as a whole.

- Education of individuals, both citizen users and staff, about risks and how to manage them ;
- Ensuring there are appropriate laws in place particularly where privacy risks are very high (for example, specifically limiting use and disclosures, providing criminal penalties for misuse if necessary) and providing special measures to manage change;
- Technology (for example, limiting information collected and who has access to it);
- Governance, including transparency and accountability (this can be a combination of policy, procedure technology and law and will often rely on technology to produce audit information);
- Safety mechanisms for citizen users when systems or services fail.

Such a layered defence approach is applicable at the local, national and global context. It goes without saying that implementing these mechanisms in a global context adds another layer of complexity. To start with governments are only just coming to terms with the implications of managing identity in a global context. The work of the OECD and APEC to put in place a global governance framework for the transborder flow of personal information is just the tip of the iceberg. Commercially developed federations of identity are contributing, but a major question remains as to whether this is sufficient.

John Harrison

- Improvements in computing and networking technology have given malign – and even some benevolent – organisations the tools to amass detailed profile information about individuals. This poses a severe threat to privacy.

[16] For further development of this analysis see a white paper called 'Safe to Play' which Information Integrity Solutions wrote with Cisco, available at www.iispartners.com/Publications/index.html#Yr2007

- To solve the problem there is a need to equip individuals with online tools that will allow them to (i) sign on, with an appropriate degree of security, to multiple distinct counterparties: and (ii) give explicit permission for the transfer of personal attributes between counterparties. A basic premise of such tools is that the individual should be known, at the relationship level, to each counterparty by a different pseudonym, thus preventing linkage of accounts without permission.

- This is the field of 'user-centric identity & personal information management' (UCIPIM), and can be seen as a subset of the broader field of Privacy Enhancing Technology (PET).

- UCIPIM tools may be located either on an individual's personal device, or on a web-server, or on a combination of the two. Microsoft's Infocards initiative is located on a personal device, but has failed to gain much market traction, arguably for lack of a clear business justification and route to market. OpenID, a server-based initiative, is supported by many large web-based organisations as 'identity providers', but their unwillingness to consume identity assertions made by others is evidence that this scheme too lacks a business model and a clear route to market. Similar comments could be made for other schemes, such as Project Higgins.

- Thus the issue hindering progress in the UCIPIM field is not technical, but rather one of working out how to drive feasible technology to the point where network effects - rather than being a barrier to adoption - become an engine for growth. A solution requires a credible application route-map and appropriate business and organisational models.

- In 2008 I led a Work Group on UCIPIM, which was kindly sponsored by the Information Commissioner's Office, the Technology Strategy Board, and the Cyber Security KTN. A copy of the group's report is available.17 By way of summary of the findings:

- Although models for UCIPIM that include a server-based element are necessarily imperfect in terms of individual privacy and control, they offer significant advantages in terms of back-up, synchronization across devices, and secure authentication. These advantages probably outweigh the privacy deficit – which, in any case, can be mitigated by good design.

- Future UCIPIM schemes are likely to feature a stepped approach to both authentication and (legal) identification, thus catering for applications requiring a range of different security levels.

- The likely business model for UCIPIM is 'service-provider pays' with some scope for individuals to pay extra for enhancements to a basic 'free' service.

- Future UCIPIM schemes are only likely to prosper if adequate attention is paid to governance. Issues that would need to be addressed include: equivalence of different authentication mechanisms; structures for exchange of payment and liability, co-branding; and account portability.

Iain Henderson: The Emerging VRM Market

VRM is an emerging (mainly) online market, the culmination and focus of many years of thinking around user-driven applications and services that aim to be truly on the side of the individual. VRM stands for Vendor Relationship Management and is the reciprocal of Customer Relationship Management – think of it as "flipping" or turning CRM inside out. It puts the individual at the centre of his online commercial world and gives him new tools and services to improve his online commercial experiences and to help him utilise and share with selected companies his personal information to improve his buying experience and his buying power and to save him time and hassle. It aims to give the individual a more equal

[17] See http://www.ktn.qinetiq-tim.net/resources.php?page=rs_ktnpublications

weight in the online market-place, and to help markets work better for *both* vendors and customers – in ways that don't require the former to "lock in" the latter.

Companies who are willing to change their mindset and engage actively with this new world stand to benefit greatly from information volunteered and shared by individuals – to increase the value and relevance of their products, services and customer information and to reduce the time, money and effort wasted in inefficient "hit and miss" communication and "broken" customer relationship management.

Mydex (www.mydex.org)

1. Mydex is a social enterprise whose charter is to 'help the individual realise the value of their personal information'. We believe that a highly regulated, Community Interest Company approach is required to generate the necessary trust amongst individuals to begin the build strong information management and sharing capabilities on the side of the individual.

2. Our view is that the current ways of working around personal information are structurally broken (organisations in both public and private cannot do other than gather and use personal information to the maximum extent allowable), and that alternate, more balanced and respectful models need to be considered and developed. We believe, that when such models are deployed, considerable new value will be released (better information, flowing in more efficient 'lean' ways'). Current legislative approaches to privacy and data protection are architected around putting the brakes on what organisations can do, rather than building the tools that enable the individuals to accelerate their capabilities.

3. Mydex will enable the individual to say, 'my view of me' is vastly superior to any other view of me; where proof is required I can bring that proof; my view of me looks forward, organisational views of me look backward'. Give me the necessary tools, incentives & protections and I will share that view with organisations which respect the terms & conditions I set around that access.

4. Those organisations that don't wish to engage in that more respectful manner can carry on scraping around for what they can patch together.

5. In other words, we say to organisations...'you currently spend, say £3 per year to access a pretty poor quality, pretty toxic record; why not spend £2 per year and change your processes to access one that's both better in depth and quality, and much less toxic'.

6. In order to access this rich information, organisations 'sign' the individuals terms and conditions rather than the other way around, and each information share generates an audit file. Compliance processes and trust-marks will be used to ensure adherence to agreements.

7. We call this concept 'Volunteered Personal Information', and this is what opens up the ability to create new value, and which will ultimately lead to a more balanced and much more efficient approach around the management and sharing of personal information.

8. We currently have a proof of concept in place using a number of high-end, open standard, secure technologies in novel ways, an open working group developing the technical standards, and a legal team working on the Volunteered Personal Information agreements (which use the Creative Commons approach as a start point – human readable, machine readable and lawyer readable variants). Our focus is not on

amending existing terms and conditions, it is on offering an alternate model that we would expect to be more economically attractive for all parties in the mid term.

9. We plan to launch a pilot service later this year based around a 'change of address scenario'. Change of address is a good illustration of the underlying premise; clearly the individual is the most informed source for that information, verification can be done relatively easily, and there is a clear logic for both individual and organisation in making the process as painless as possible.

10. Change of address is a natural forerunner to change of other contact details and other changes of circumstances. In enabling these user-driven information sharing capabilities we open up the route towards the individual being the integrator of a much wider array of personal information relating to them.

11. Moving beyond ‘useful’ sharing processes, information on future buying intentions represents the inevitable shift from useful information towards higher value volunteered personal information sharing that will be enabled by Mydex and others. This offers the potential to eliminate much guesswork and waste in the marketing services and advertising industries and ultimately enables a much closer relationship between demand and supply with all that this entails.

12. Over time, the personal data store(s) of the individual will become rich analytical systems in their own right, enabling the individual to make better decisions relating to their circumstances and informed by the many other accessible information sources on The Internet.

Ronald Leenes: Legal interoperability in pan European authentication

The EU co-funded STORK project[18]aims to make it easier for EU citizens and businesses to access online public services across borders using their national electronic identities. The STORK consortium includes a total of 29 members composed of national governments, academia and research, non-profit and private organizations. The project builds on existing eID solution and tests and develops common specifications for mutual recognition of national electronic identities (eID) between participating countries. Part of the STORK project is an analysis of the technical and legal issues in the field of eID interoperability in 14 STORK member states.[19] The current brief is based on this legal analysis. When discussing interoperability of eID in this deliverable, we refer to the 'formal' electronic identities, which are the identities that are constructed out of identity information (attributes), and are recognized by national governments, for application (especially for authentication) in national eGovernment services(and sometimes in private services as well). Such formal identities are usually provisioned by (central) authorities and may consist of soft tokens and/or be stored on smart cards or other devices. In the light of pan-European service delivery, it is useful to distinguish between entity authentication and attribute authentication. By entity authentication we mean: ‘the assessment whether an individual is who (s)he claims to be’. Usually this process results in an identifier associated to the authenticated individual such as a name and/or some identifying number provided by an authentication authority.[20] Usually also a number of attributes associated to the authenticated individual become available as a result of entity authentication, particularly in the case of smart card based identities which include X509.4 certificates. Attribute authentication relates to the question: ‘does individual X really have attribute Y?’ For instance, is X a student enlisted in a Dutch institute for higher

[18] INFSO-ICT-PSP-224993, see http://www.eid-stork.eu/

[19] AT, BE, DE, ES, FR, IC, IT, NL, LU, PT, SL, SE, UK.

[20] Which may, but not necessarily, be a Certificate or Certification Authority

education, or does Z really live in Prague. Entity authentication is a special case of attribute authentication (namely one where the question, for instance is: is X's name really X?), but for practical purposes it may be useful to distinguish the two.

Prevalent forms of authentication are username/password authentication by a public authority and (qualified) certificates which either consist of soft (X.509) certificates or hard certificates when embedded on smart cards. Username/password combinations are used in many member states, especially for low risk services. Most often, username and password are associated to e-IDs created in the context of a particular service, e.g., Iceland where many government services have their own eIDM system. These are impractical for PEGS precisely because they are associated to a particular service provider. Some member states have portals (usually federated identity management systems) that handle the authentication of citizens for a number of services. Examples are the Dutch gbo.Overheid (DigiD), the UK Government Gateway and the French mon.service-public.fr. These systems pose either practical problems with respect to pan-European public service delivery, or suffer from legal barriers in relation to PEGS. The UK Government Gateway could in principle handle the log-in of UK citizens for foreign services, but this would require each relying party to sign up for the Gateway, which is rather impractical.

The legal framework in which pan-European authentication and Pan-European eGovernment Services (PEGS) operates, includes regulation on the EU level, as well as national regulation in the various member states. The latter includes public law as well as private/civil law (think of liability issues). Pan-European authentication involves personal data and hence the Data Protection Directive (95/46/EC) applies. A central requirement in this context is art. 7 of the Directive are met (legitimate ground). Unambiguous consent of the data subject (the claimant) is the most likely ground for data processing regarding PEGS given that a legal obligation (as meant in art. 7(c)) is unlikely to be present in a pan-European context. Consent can easily be obtained when the data is disclosed by the claimant herself (e.g., in an online form), or when data can be obtained from a certificate presented by the claimant (e.g., a smart card presented by the claimant). This is different when the service provider (relying party) requires additional data, such as (certified) attributes and cannot be obtained from the claimant but have to be obtained from sources such as authentic registers in the claimant's home state without the claimants' involvement. In these cases, the relying party still would have to ask the claimant's consent in order to make the processing legitimate. Special attention needs to be paid to the article 8(7) pertaining to national identification numbers and other identifiers. Many eIDs contain identifiers that are based on, or are equal to, national identification numbers (e.g., Estonian Personal Identification Code, Dutch BurgerSeviceNumber, Spanish DNI number). In most countries, the use of these numbers is regulated by law, and in fact in most cases restricted to use within the member state. The Dutch BSN, for instance may only be used by authorized entities that are listed in the Act on the Citizen Service Number, all of which are within the Dutch jurisdiction which limits the use of the BSN to Dutch (e)Government interactions. In some countries identification numbers may be processed (even abroad) if the data subject consents (e.g., Estonia, Italy, Spain). Germany does not have national identity numbers, but instead uses combinations of other attributes such as name and date of birth as identifier for individuals.

The eID's differ in the amount and nature of the attributes they contain. On the one extreme there are 'lean' eIDs, such as the Dutch DigiD, which only contains the 9 digit identifier BSN. On the other extreme there are 'rich' eID, such as the Portuguese Cartão de Cidadão which contains Name, date and place of birth, date and place of issuance of the card, validity period of the card, parents, marital status, title and number of the card, picture and handwritten signature, residence, and National register number, the holder's address and two digital certificates, one for identification and authentication and one for a qualified electronic signature. In the latter case, some of the attributes represent authentic and accurate data (e.g., date of birth), while other data may require further proof or validation (e.g., even name may not be stable, think for instance of married women who may adopt their husband's surname in a number of EU member states). Many eIDs do not contain the nationality of the holder, although country of issuance is an attribute present on all eID cards. Whether the eID’s attributes may be used in PEGS varies per member state.

Some member states have authentic registers that offer authorised entities access to authentic citizen data. At least Austria, Belgium, France, Italy, Iceland, Luxembourg, Slovenia, the Netherlands and Sweden, have extensive authentic registers that can be consulted to verify or obtain up to date attributes. The access regimes to these registries differ significantly between the member states. In some case the register is open to consultation by anyone, in other cases access is completely confined to authorized entities (e.g., Estonia where everyone with an ID-card can access the X-road register), or even entities mandated by law (e.g. the Netherlands where access to authentic registers is regulated by law). Some authentic registries are open when a 'Memorandum of Understanding' exists between the relying party and the authentic register (or the responsible government actor), as in Italy, or when a contract exists between Relying party and authentic register (e.g., Iceland, Sweden).

The e-Signatures Directive (1999/93/EC) is relevant because it pertains to certificates, which are used in the various eIDs in the STORK member states. Many (smart card based) eIDs include a certificate for authentication and another for digital signatures. All authentication certificates, by definition, can be used to authenticate the (confirm the identity) of the holder. Qualified certificates provide a higher assurance level than other (advanced) certificates because they are issued in a more tightly controlled process. Because of these requirements, users of QCs may expect verified certificates to meet particular quality requirements regarding content and validity and hence CA’s issuing Qualified Certificates have a certain liability as described in article 6 of the e-Sig Directive. Qualified Certificates can be used for different functions (authentication, signature, etc); the Directive is indifferent in this respect. It is up to the individual member states to determine whether they accredit certification-service providers and give them the right to issue qualified certificates and whether their eIDs make use of qualified certificates or other certificates. Some countries use qualified certificates for their eID's (e.g., Austria), others don't (e.g. Belgium for the authentication certificate). This may lead to difficult liability issues because the liability in the case of QC's rests on the CA that issued the certificate, whereas this is more complicated for non qualified certification-service providers. These are likely to have provisions (waiving) regarding their liability in their terms of service. Because there are potentially many certification-service providers this may lead to a complicated mesh of different liability regimes.

Differences exist in the way an entity can obtain eIDs in the various member states and therefore who can obtain authentication certificates. Also the use of these certificates is regulated. Some member states promote the use of certificates in order to create trust in online transactions and this may include posing very few restrictions on using them in pan-European eGovernment transactions. Differences also exist in who may verify authentication certifications by means of OCSP and CRL mechanisms. This depends on the conditions imposed by the different CA’s, but also on national regulation within the various member states. Some CA’s, for instance require prior contractual agreement with users of verification services.

This brief summary shows that the legal landscape of pan-european authentication for PEGS poses significant challenges for implementing PEGS on the basis of the existing eIDs and regulatory frameworks.

David Lello

Introduction

In IT, it is always said that it is about people, process and technology. This principle holds true with successful Identity projects. It can be seen that a direct correlation to a greater effort been applied to Process and People (Business Change) has resulted in success.

Identity Management is a fundamental principle of good governance, in any organisation, and must be seen as such. If this principle is accepted then the basis for any discussion should start with alignment of exiting operational risk legislation or standards: Sarbanes Oxley; Basel II; or CobiT; etc.

While these regulations and standards start the process they may be inadequate, or are they? If inadequate then building on these areas of legislation, specific standards must be considered. Perhaps it is not about new legislation, but rather about acknowledging existing and offering only a policy framework to help organisations succeed.

The areas I would like to highlight are: and Effective Framework; Reporting; Functional Inclusions.

Caution

Identity can be easily manipulated to invade on civil liberties in a negative way, consideration of this must be made.

1. Framework

Implementations of Identity have resulted in may failures due to technology driven projects and novices wanting a piece of the pie. As a function of any legal framework in this space it is most important that a phased approach with levels of compliance be considered. Specific guidance on the change impact of such compliance must be made.

Identity Management and all of its functions and features including Access Management are complex for one reason: That being that a fundamental change is applied to the organisational procedures. To make matters worse these procedural processes are applied to the majority of technology systems, all with traditionally disparate processes.

To ensure that a legislative framework of this nature is widely accepted it must allow for a staged approach with levels of compliance and within a reasonable time frame. Emphasis must be put on what controls are required, how and when they are to be implementation.

2. Reporting

Measurement and Reporting is without debate key to recording compliancy. I would caution how criteria are tabled as companies are already overburdened with compliancy reporting.

It would be appreciated by risk officers that standards such as CobIT are used or at the leased to consider what companies may be reporting on based on SOX, etc.

A policy framework must clearly define what evidence is required and what the guidelines are for how this must be affected.

The measure of success and need for case law with irrefutable evidence must be the basis of any reporting capability. If it cannot stand up to this singular principle then it is impotent and useless.

3. Functional Inclusions

As Identity Management has become broad by nature it is important to be clear as to which components of Identity Management must be excluded, or at least deemed voluntary.

Many functional elements exist in the formation of Identity Management Projects, some of these components can be onerous or even ineffective in supporting regulatory principles.

Some functional elements are ineffective security mechanisms, such as Single Sign On, where in itself it is counterproductive to good security principles.

Other functional areas would be extremely difficult to enforce, such as fully automated provisioning, as many proprietary systems are not supported by current technologies.

Distinction must be made in the extent of use, such as where Role Management tools are very useful in aggregating and cleansing user data for Identity. On the flip side definition of functional roles can be very subjective and based on several factors.

Provision should be made on how to enforce Identity components where some levels of outsourcing is applied, especially with federation.

Functions need to be identified, definitions applied, its viable application of effective use discussed, specifically as a tool for case law. Only areas that are practical and that can be enforceable should be discussed.

4. Next Steps

First and foremost we need to understand if further compliancy is required over and above what is required already.

In appreciation for the successes that we have seen in industry. A framework needs to be documented clearly indicating what must be done, how it should be achieved and in which timeframe controls are to be enforced.

Each functional component of Identity Management must be: listed; defined; its effectiveness ascertained; validation of potential for enforcement; definition of use within legislation; and its inclusion or exclusion confirmed.

More than ever Identity Management must be appreciated as a business process issue with technology offering enablement.

Jan-Martin Lowendahl, Gregg Kreizman: Governments Need and Can Play a Role in the Online Claims Ecosystem

Growing numbers of stakeholders agree that "identity is the missing layer of the Internet." Lack of convenience, privacy, interoperability and international policies hamper the development of the networked economy. Government has a role to play in building the identity ecosystem needed to ensure trust in transactions.

Overview

The "identity problem" has to be solved in order for the networked world to reach its full (economic and democratic) potential. Governments bear a heavy load in the responsibility of building a sustainable identity ecosystem, but all CIOs and IT software and service vendors need to know how an identity ecosystem with multiple identity attribute providers will impact them.

Key Findings

- Lack of a more-distributed identity ecosystem is propagating inefficient, insecure, silo-based identity infrastructures, and is a limiting factor in establish trust in transactions.
- Governments have several roles to play in improving the identity ecosystem.

Recommendations

- Governments should facilitate issuing and verifying basic identity attributes like nationality, name and birth date by investing in citizen-centric systems
- Governments should be heavily involved in developing and supporting policies such as levels of assurance (LOA) that clearly outline the risks associated with using identity attributes in different contexts and how attributes are issued as well as how breaches of these policies will be handled by law.
- Governments should be heavily involved in developing identity and access management (IAM) standards, such as SAML and OASIS Identity Metasystem Interoperability.
- CIOs that need a working IAM solution that extends beyond the organization today should implement a standards-based federated solution with a focused community of interest to ensure a minimum of disparities associated with LOA and identity-attribute sharing differences, and a maximum business case for joining up.

Introduction

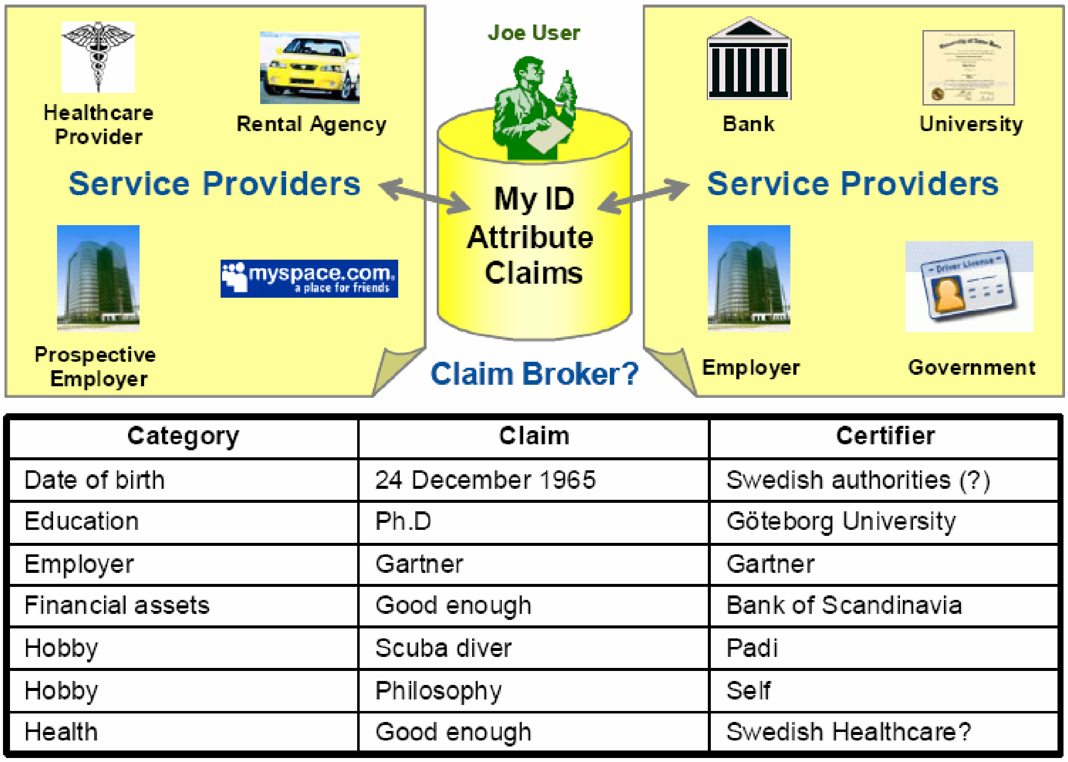
Results from workshops such as the Organization for Economic Co-operation OECD workshop "Digital Identity Management" (see www.oecd.org) and the Oxford Internet Institute (see oii.ox.ac.uk) strategy forum "e-Infrastructures for Identity Management and Data Sharing: Perspectives Across the Public Sector" have confirmed that the stakeholders in the future of the networked world are many, diverse and increasing rapidly. More than 1.5 billion people now have access to the Internet, and they are increasingly dependent on it for commercial and official transactions as well as personal relationships. In this networked world, ad hoc or siloed approaches to handling identity and related attributes lead to inappropriate and inefficient practices when managing identity data and constituent authentication practices. The concept of an identity ecosystem has been promoted to address this, and this research explores the potential role of governments in developing or encouraging the development of that ecosystem, and what chief information security officers (CISOs) can do now to prepare for its emergence. Privacy issues and outright fraud are among the top reasons for individuals not wanting to engage in digital relations, and it is also a major concern for corporations and governments. For example: Gartner estimates that lost "goods not present" sales due to actual fraud, credits issued for transactions claimed as fraud or declined transactions that looked suspicious represent 1% to 3% of total revenue. Furthermore, about 7.5% of U.S. adults lost money as a result of some sort of financial fraud in 2008, according to a recent Gartner survey (see "Digital Commerce Fraud Challenges and Solutions" and "2008 Data Breaches and Financial Crimes Scare Consumers Away"). Lack of access to systems that verify credit cardholders' names, addresses and phone numbers plays a role in this fraud. Paradoxically the "lack of an identity layer on the Internet"[21] today increases the privacy related risks as there are few means to release identity attributes in a controlled manner. Convenience is another major issue for the development of virtual relationships, regardless of whether they are personal, commercial or official. The de facto nature of today's networked world, with its many "identity silos" or, in the best case, walled gardens of identity relations, severely hampers the development of a healthy ecosystem of service consumers and service providers. A digital service ecosystem has a whole range of benefits, including being an economic motor in the continued growth of the world economy to a potential weapon against global warming in enabling less physical travel. The critical success factors of this ecosystem from the end user's view is "transparent risk mitigation" and "convenience."

The Complexity of the Identity Concept and the Growth of a Claims Ecosystem

A fundamental problem is that the concept of identity that has been developed for millennia in real-world society is now trying to map "itself" onto the emerging networked world — with great difficulty. Many relationships that we subconsciously handle with basic biometrics in the real world (such as simply recognizing a face) now have to be explicitly coded and regulated in the virtual world — which does not have the same basic rules as the real world, where "visual biometrics" does not yet work on a global scale, and where everything is potentially traceable. Forums such as the OECD workshop and numerous blogs and conferences clearly show that the concept of identity in both in the real and virtual world can be an interesting semantic problem that will fuel philosophical discussions for decades and have very different outcomes depending on cultural, business and technical context. However, while these discussions are very important and can provide good insight into possible solutions, history has shown over and over again that a problem of this complexity needs an empirical approach. Real-life pilots in a well-defined community of interest with a detailed evaluation process offers the best chance of gathering best practices to be used for the evolution of a scalable solution. It is in this context that the concept of a claims ecosystem has been developed (see Figure 1)

[21] The phrase "identity is the missing layer of the Internet" has become a catch phrase and a concise way to state the "identity problem" in the community that engages in identity-related questions. An example is how Microsoft's Chief Architect of Identity, Kim Cameron, introduces the identity problem that led to the community developed "Seven Laws of Identity" (see http://www.identityblog.com/?page_id=354): "The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception that will cumulatively erode public trust in the Internet."

Figure 1. The Big Picture: Where Do You Fit Into the Claims Ecosystem?



Category	Claim	Certifier
Date of birth	24 December 1965	Swedish authorities (?)
Education	Ph.D	Göteborg University
Employer	Gartner	Gartner
Financial assets	Good enough	Bank of Scandinavia
Hobby	Scuba diver	Padi
Hobby	Philosophy	Self
Health	Good enough	Swedish Healthcare?

Source: Gartner (March 2009)

A claims ecosystem bypasses the complexity and the emotional and philosophical issues attached to the current definition of identity, and focuses on certifiable claims made by individuals or organizations. The fundamental principles of the claims ecosystem are a user-centric approach together with relational relevance. We'll use a real-world example to explain the principles:

Renting a car involves at least two fundamental claims:

- The rental agency needs to know if you have a valid license to drive a car (because the law demands it and because the rental agency want to minimize the risks that you crash the car by showing that you have passed some sort of driver's test). This claim is in most countries supported by a government associated agency.
- The rental agency needs to know if you have the money to pay for the rental of the car. This claim can be supported in many ways, most commonly by cash or a credit card where you show you have control of the money by possessing the card, and perhaps knowing a PIN so the card issuer verifies that the holder can pay.

In principle, none of the above claims demands that you divulge other personal information such as name, date of birth or home address. However, most rental agencies demand that kind of information too in order to mitigate the risk of you stealing the car or disappearing if there is an accident.

Similarly, most transactions and relations involve a step where the individuals involved represent themselves with a key individual identifier, such as a name verified, for example by an ID card (it does not have to include a name; anything that ensures traceability and accountability will do). Then, the transaction proceeds by one party asking for a service, presenting claims that must be verified by a relevant third party; for example, an educational degree verified by your university, or health status verified by your physician (see Figure 1).

The key for all the service providers, service consumers and claim certifiers is to find the lowest common denominator to enable cost-effective interoperability. That this is not just a technical issue can be illustrated by the example of the road transportation system. Over time, most road systems around the world have adapted to certain technical standards and business needs that enable the global use of cars. The roads are of a certain breadth, gas station are at certain intervals and cars must be of certain dimensions. However, in most countries, this is not enough. In order to mitigate the risks of driving vehicles, there is license plate identification and driver's licenses that certify basic education in the rules of engagements on the road (traffic laws). Highway police enforce the laws, and traffic courts ensure that individuals are held accountable for their actions. On an individual level, this system enables simple, sometimes life-preserving courses of action, such as: I do not trust a driver in a car without a license plate, so I mitigate my risk by staying as far from that car in traffic as I can.

This kind of integrated societal infrastructure (technical and legal) can often have many second order effects that catalyze the economy, such as greater areas available for jobseekers and competency hunters due to commuting, and a global industry providing cars, gasoline and insurance. Even more interesting are "third-order" effects such as when a commonly accepted means of identification such as the driver's license in some countries can be used to open a bank account or prove legal age for buying alcohol. These financial transactions would not have been possible without a generally accepted means of providing certifiable claims, which in this case are totally unrelated to the original purpose of the use of a driver's license. This is a prime example of how a good claims ecosystem can catalyze economic transactions simply by convenience and at the same time save time.

Of special interest is the key to this "third order" effect: the level of assurance (LOA) I can put in a driver's license. In many countries a driver's license or a passport can only be issued in person by providing a means of identification that is traced back to a birth certificate. This is usually the highest level of assurance for basic identity attributes we can achieve in a modern society and something that explains these documents' wide use in many contexts besides their original purpose. This should be contrasted with the level of trust put in self-asserted attributes such as a business card, an OpenID or worse, an e-mail address.

Due to its general usefulness, most countries have developed a federated claims ecosystem that defines the legal validity of identity attributes such as the passport and the driver's license. Most countries require a passport to enter the country and many countries accept each others driver's licenses at least for a limited stay. In some regions, such as the European Union (EU) Schengen area, driver's licenses are accepted for international travel in the name of facilitating economic development within an economic zone. These third-order effects have a downside, too. As these identifiers are used outside their originally intended ecosystem, they can divulge information that is contrary to the "constrained use" principle. This has, for example, the effect of increased risk for fraud and potential privacy infringement. This has led to state laws in the U.S. to limit use and storing of driver's license data. This is a good example of the need to modernize the claims ecosystem to include the demands of the digital networked world.

The government Role in the Digital Claims Ecosystem

Since most governments today play a significant role in many important traditional claims ecosystems, it is very likely that governments will be relied on for analogous functionalities in the digital claims ecosystem, especially in the international context. Governments have the experience in and responsibility for many societal infrastructures that ensure trust and accountability in financial transactions and social relations. This know-how will be instrumental in building digital equivalents. However, their roles in the claims ecosystem vary greatly in different nations and cultures and must be adapted from the bottom up to allow for true technical and legal interoperability.

For governments to step up to this task, they need to:

- Facilitate issuing and verifying basic claims such as nationality, name and birth date by investing in citizen-centric systems. Ideally, governments would be at least one of these issuers of basic credentials per jurisdiction. This is comparable to the role of issuing passports and ID cards in most countries.
- Be heavily involved in developing and guaranteeing policies such as LOAs that clearly outline the risks associated with an identity attribute and how it is issued as well as how breaches of these policies will be handled in a court of law (that is, punishment and liability for damages).
- Be heavily involved in developing Identity and access management standards, such as SAML and the OASIS Identity Metasystem Interoperability so that the same claims ecosystem is useful (secure, cost-effective and protective of integrity) for government services as well as third-order services. A key for the claims ecosystem to be successful is to handle not only high-level LOA claims or seldom occurring claims, but also lowlevel LOA claims and frequent claims. The former which includes, for example, claims used in tax returns has a very different business case in terms of acceptable cost per transaction than the latter. Examples of the latter is access to a building or where the cost per transaction has to be very low since it can be invoked several times a day. However, in both cases the key can be a "person identifier" such as a name claim.

What Are the Implications for CISOs and CIOs?

A fundamental question is what the practical implications of a claims ecosystem would be. How should IT services be designed and delivered? What security risks are involved? What are the legal risks?

The first consideration is what technical strategy will succeed in providing the missing identity layer of the internet. Currently, there are three basic approaches under consideration today: organization-centric versus federated versus user-centric.

The organization-centric approach has already shown a high rate of failure both in the government and commercial sector due to reasons of lack of interoperability and privacy. Most importantly citizens and consumers simply do not trust centralized systems. The most highprofiled failure is probably the Microsoft Passport service (see "Consumers Don't Want to Change the Ways They Manage Passwords Online").

The federated approach is relatively recent, but there are examples of successes in well defined communities of interest. Embryos of healthy ecosystems can be seen already today in the education sector, where large-scale federated identity systems enable interorganization service sharing and also have prompted service providers, such as publishers, to develop new services targeted for the education community. For the service providers, the incentive is lower cost of distribution, shorter time to market and access to a wider market. Software as a service (SaaS) providers are also offering federation interfaces to enable authentication to their services, and a market for SaaS IAM gateways is emerging to help enterprises leverage enterprise IAM infrastructures when provisioning and authenticating to SaaS providers (see "SaaS IAM Gateways Begin to Take Hold, and New Solutions Join the Market").

The approach that has shown the most promise for the future and that really builds on the proven decentralized approach and the success of the Internet itself as well as lessons learned from federations is "user-centric identity." Insights gained from the Microsoft Passport failure that resulted in the Seven Laws of Identity"[22] and the early successes of OpenID for low assurance needs suggests that there is much potential in this approach. Many stakeholders are involved in policy efforts, standard efforts and efforts to provide technical solutions.

On the policy side, examples include the OECD interest in developing government policy guidelines and the Information and Privacy Commissioner of Ontario's work on mapping of the Seven Laws of Identity' onto its "Fair Information Practices" (see www.ipc.on.ca and www.csa.ca/standards/privacy). On the standards side, examples include the work that the Liberty Alliance is doing on interoperability with a user-centric model. Providers of technical solutions are many. Some of the main players include and Microsoft with its CardSpace solution, IBM and Novell in collaboration with many others with the Higgins framework and OpenID's "community" approach.

Much progress has been made with the user-centric approach that has advanced the state of "digital identity," especially in the area of privacy. However, this approach is heading towards the Trough of Disillusionment, predominately due to problems with "Law 1 of the Seven Laws of Identity: " User Control and Consent: Identity systems must only reveal information identifying a user with the user's consent". There is often an overly strict interpretation of user consent and ownership of identity-related data that has its roots in philosophical discussions and political views on what identity is, and leads to entrenched positions. Furthermore, some of these user centric views are not compatible with how government agencies and health care organizations need to handle identity-related data.

As we point out, the user-centric approach can be evolved by introducing a claims-centric ecosystem instead. A focus on concrete, verifiable claims or at least a means to asses the risk of those claims not being true by knowing how they are verified (for example self-asserted or government-asserted claims) can lead to practical, useful solutions.

If this approach succeeds, it means that both CIOs and vendors of software and IT services will have to be prepared for technical and legal environments where all identity attributes are not validated or owned by their own organization. They will have to find their role in the digital claims ecosystem.

However, while waiting for the government to step in, CIOs that need a working IAM solution that extends beyond the organization today should implement a standards-based federated solution. The best approach is to start with a focused community of interest to ensure a minimum of disparities associated with needed LOA and identity-attribute-sharing differences, and a maximum business case for joining up. This will enable immediate benefits and prepare the organization for many aspects of the digital claims ecosystem.

Recommended Reading

"Lessons Learned From Higher Education and Public-Sector Identity Federations"

"Identity and Access Management Is Key to European Academic Mobility"

"Case Study: Is Norway's FEIDE a Step Toward a National IAM Solution?"

"Developing IAM Best Practices"

"The State of IAM in Europe"

[22] Ibid.

"Hype Cycle for Identity and Access Management Technologies, 2008"

"Fellows Interview: Gartner's Interview With Identity 2.0 Thought Leader Kim Cameron"

"Identity 2.0: Tomorrow's Promise and Today's Reality"

"The State of User-Centric Identity, 2H08"

"Consumers Don't Want to Change the Ways They Manage Passwords Online"

"Digital Commerce Fraud Challenges and Solutions"

"2008 Data Breaches and Financial Crimes Scare Consumers Away"

Lucy Lynch: Trust and Identity

The Internet Society's Trust and Identity initiative recognises that in order to be trusted, the Internet must provide channels for secure, reliable, private, communication between entities, which can be clearly authenticated in a mutually understood manner. The mechanisms that provide this level of assurance must support both the end-to-end nature of Internet architecture and reasonable means for entities to manage and protect their own identity details.

A trusted Internet takes into account security, transaction protection, and identity assertion and management. Given the network dependence on unique numbers and the escalating amount of both personal and geolocation data being gathered, the privacy implications of the current Internet represent a significant and growing concern. Trust must be a primary design element at every layer of the architecture, and in some cases, existing elements may need to be redesigned or improved to meet emerging requirements.

The ISOC Board of Trustees conducted a three-day retreat in October 2007 in Toronto to focus on the subject of trust within the context of network-enabled relationships. The Trustees determined that the issue of trust is both important and crucial for the long-term growth and success of the Internet. After a review of current literature and of emerging research efforts as well as consultations with subject experts, the following areas were deemed to be of special importance:

- Advancing Internet architecture by supporting the implementation of open trust mechanisms throughout the full cycle of research, standardization, development, and deployment
- Strengthening the current Internet model by focusing on the mitigation of social, policy, and economic drivers that could hinder development and deployment of trust-enabling technologies
- Facilitating end users' ability to manage personal data and ensure personal security by elevating identity to a position as a core issue in network research and standards development

As a result of this investigation, the Board of Trustees approved Trust and Identity initiative focuses on the following major research programmes[23].

[23] See: "Trust and the Future of the Internet" http://www.isoc.org/isoc/mission/initiative/docs/trust-report-2008.pdf

- Identity and Trust: This research programme investigates the elevation of identity to a core issue in network research and standards development. ISOC is taking a lead role in reviewing the current Internet architecture and the model of Internet development and deployment. This includes active engagement with participants within the traditional ISOC sphere, as well as with the research, enterprise, and end-user communities. We offer direct support for research that enhances and facilitates trust. ISOC also encourages collaboration with the standards communities that advance the outcomes of that research.
- Architecture and Trust: This research programme investigates the implementation of open-trust mechanisms throughout the full cycle of Internet research, standardisation, development, and deployment.
- Operationalizing Trust: This research programme investigates the mitigation of the social, policy, and economic factors that may hinder development and deployment for trust-enabling technologies.

ISOC is reaching out to the businesses and end users that rely on the Internet to exchange sensitive data. Their needs and concerns inform both our baseline research agendas and ongoing standards and development work. ISOC continues to support the advancement of current technical solutions and best practices through our existing programmes.

Our major focus in 2009 will be on Identity as we seek to educate end-users on the critical importance of user managed identity. A secondary focus on current trust enabling protocol efforts will establish the basis for Architecture and Trust work which will take center stage in 2010.

Network Confidence

ISOC seeks to establish a clear distinction between a trust enabled network and network security. We will provide reliable information on trust enabling network technologies and will illustrate the importance of network trust as the long term solution to the issues that underlie many of the current concerns about cyber-security

User Managed Identity

ISOC is seeking to elevate "Identity" to a core issue in network research and standards development and to ensure that user education regarding identity management is seen as vital to creating a trusted Internet. To that end, ISOC will publish a public report in 2009 based on a broad consultation with representatives from the Identity technology communities, ISOC members, the IETF, and the IAB. This report will focus on “User Managed Identity” and will be addressed directly to end-users. The consultation process will serve to build an on-going relationship with identity experts and the published report will be leveraged to open a dialog with end-users.

Meryem Marzouki: The “Guarantee Rights” for Realizing the Rule of Law

When addressing the global issue of human rights in the information society, and how these rights may translate in such a context, one immediately thinks of civil and political rights that should be directly and naturally exercised through information and communication means, or protected against their misuse.

These obviously include the right to freedom of expression and to seek, receive and impart information, the right to access public information and to take part in the conduct of public affairs, and the right to privacy.

Then, following a vision of an inclusive information society where all categories of individuals, social groups, minorities and peoples should have access to information and communication - where access not only means access to infrastructure but also appropriation and use of technology for empowerment and social justice - come issues related to non discrimination, such as the right for men and women to equally enjoy all rights, rights for minorities to enjoy their own culture and to use their own language, the right to education and knowledge and to participate in the cultural life, to enjoy the benefits of scientific progress and its applications, the right to development and the principle of non-discrimination itself.

Furthermore, in an extended understanding of the concepts of association, assembly, movement, etc., the right to freedom of peaceful assembly and association emerges as an issue to be addressed in this context too.

However, despite intense regulatory and legislative processes occurring for almost a decade at the national, regional and international levels, and despite many references to the rule of law in official outcomes of the first phase of the World Summit on the Information Society (WSIS) in Geneva in December 2003, fundamental human rights like the right to a fair trial, the right to the presumption of innocence, the right to an effective remedy, the right to equality before the law, and the principle of no punishment without law are seldom if ever addressed in the information and communication context.

The purpose of this chapter is to provide rationale to the legitimate inclusion of these rights in the debate on human rights in the information society, showing how, as “guarantee-rights”, they are necessary conditions to the realization of the rule of law and thus to the effective enjoyment of all other human rights ; how they have been particularly challenged by regulatory and legislative processes that make procedural rather than substantive changes in the legislation ; and, finally, how these rights may be upheld and effectively implemented in the information society.

Identity control, activity control: from trust to suspicion

Processes introducing biometric identity control and communicating activity controls through data retention sign, in France and Europe, a reversal of perspective. Taking into account the legislative and regulatory transformations as well as the strategies of government and industry actors, and considering the various means of consent from the general public, we will analyze several levels of this change of paradigm: security objectives centered on intelligence rather than legal investigation; legislative and judicial proceedings oriented towards soft and contract law; intervention of private actors with prerogatives of public power; preventive rather than repressive civil or penal actions, specially through the use of technical means; sometimes inversion of the burden of the proof, requiring proving innocence rather than guilt. This results in the change from a conception of society based on mutual trust into a situation of generalized suspicion.

Gregory Neven: Requirements for a Privacy-Friendly Access Control Language

Abstract

This brief sums up a number of privacy-enhancing requirements for access control policy languages, with a special focus on supporting the advanced features of anonymous credential technology. A language satisfying these requirements, amongst others, is currently being developed by the European project PrimeLife.

Introduction

An access control policy specifies which entities are allowed to access a particular resource. Entities can be natural persons, but could more generally also be systems or running processes. Resources could be a physical resource, like a printer, but we focus mainly on digital resources such as database records or web services. One of the main focuses of the research project PrimeLife, funded by the European Commission's 7th Framework Programme, is the development of a privacy policy language that encompasses a powerful access control language. A full (draft) list of requirements was made available to the public [PL08], we summarize a selection of them here.

Requirements

Credential-based setting. As the main basis for evaluating access control decisions we consider the value of attributes as stated in *credentials* held by the entity. Credentials are essentially authenticated lists of attribute/value pairs, that are issued by a trusted issuer to the bearer of the credential. Credentials can be of different types, which define the attributes that they contain. For example, the government may issue passport credentials that contain a natural person's name, address, and date of birth. A bank may issue credit card credentials that contain the name of the holder, the credit card number, and an expiration date.

Technology independence. The policy language should make abstraction of the particular technology that is used to verify the validity of the credential. That is, credentials could be authenticated using X.509 certificates, Kerberos tickets, trusted LDAP directories, or using Idemix [CL01] or U-Prove [Bra99] anonymous credentials.

Atomic credentials. Credentials form atomic groups of attribute-value pairs, in the sense that attributes from one credential cannot be confused with attributes from another credential. This is particularly important when one entity can own several credential of the same type. For example, if the access control policy asks to reveal the number and expiration date of a credit card, then a user with two credentials should not be able to satisfy the policy by revealing the number of one credit card and the expiration date of the other. In general, attributes are only assigned to entities through credentials. Entities do not intrinsically “have" attributes, they only “possess" credentials that contain attributes.

Data minimization. The policy language should distinguish between attribute values that have to be revealed (e.g. name, credit card number) in order to gain access to the service, and the conditions that those or other attributes have to satisfy (e.g. age>18, expiry>today). For many technologies the only way to prove that attributes satisfy a certain condition is by revealing them, but this is not true for all technologies, in particular not for anonymous credentials.

Revealing attributes to third parties. When an attribute is to be revealed, it should be possible to optionally specify to whom the attribute should be revealed. For example, an online shop may specify that the credit card number should be revealed to the bank, not to the shop itself. It is up to the underlying technology layer to make sure that a third party actually did receive the required attribute value, for example by signing a receipt, or by using verifiable encryption [CS03].

Limited spending. The access control policy should be able to express restrictions on the number of times that a certain credential was used. For example, an online opinion poll may not want to know the identity of voters, but may want to make sure that no voter votes twice on the same issue.

References

[PL08] PrimeLife Consortium. Draft requirements for next generation policies. PrimeLife deliverable H5.1.1, 2008. Available from http://www.primelife.eu.

[CL01] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Advances in Cryptology { EUROCRYPT 2001, vol. 2045 of Lecture Notes in Computer Science, pages 93{118. Springer, 2001.

[Bra99] S. Brands. Rethinking Public Key Infrastructure and Digital Certificates | Building in Privacy. PhD thesis, Technical University Eindhoven, 1999.

[CS03] J. Camenisch and V. Shoup. Practical verifiable encryption and decryption of discrete logarithms. In Advances in Cryptology { CRYPTO 2003, vol. 2729 of Lecture Notes in Computer Science, pages126{144. Springer, 2003.

Viv Padayatchy: The Internet Domain Name System (DNS) and Identity Management (IDM)[24]

Introduction

The Internet is very well positioned to become the underlying medium of choice to support an Identity Management (IDM) infrastructure. An IDM infrastructure will make use of several application layers of the Internet Protocol (IP) network. For example, it might use urls, world wide web, name resolution, routing protocols, encryption etc. Therefore, as the Internet itself faces some key issues regarding its governance, it will be necessary to consider these issues in the elaboration of an IDM policy development process so as to ensure successful deployment of an IP-based IDM infrastructure and mechanism, especially in the context of the ubiquitous computing environment.

The Current Internet Governance Ecosystem

At the heart of the Internet infrastructure management are the global namespaces such as “com”, “net”, “org” etc. They are known as the global top level domains or gTLDs. The country namespaces (“uk”, “fr”, “de” etc) were added later and are referred to as ccTLDs or Country Code Top Level Domains. In parallel to the namespaces is the number space which refers to the pool of IP addresses (e.g. 196.3.111.20) which is allocated to operators around the world. The mapping of the name space to the number space and vice-versa is the basis of the Domain Name System or DNS. Today, all aspects of the management of the DNS ultimately links to the umbrella organization known as ICANN (Internet Corporation for Assigned Names and Numbers).[25]

ICANN was initially created to administer the IANA or Internet Assigned Number Authority. IANA itself was a US government funded organisation mandated to manage and coordinate the DNS. With the gradual shift of the Internet from an academic network to a commercial network, the US government stopped funding the IANA and, instead, created ICANN with a mandate to manage the IANA within the framework of a Memorandum of Understanding with the Department of Commerce.[26]

[24] This brief represents the author’s personal opinion and shall not be construed as that of Afrinic’s members, staff, affiliates or Board of Trustees.

[25] http://www.icann.org/

[26] http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm

The current structure of ICANN has four main “supporting organisations”:

- Address Supporting Organisation (ASO)
- Global Names Supporting Organisation (GNSO)
- Country Codes Supporting Organisation (CCNSO)
- Technical Liaison Group (TLG)

The ASO coordinates the activity of the Regional Internet Registries (RIR), which are responsible for allocating IP address resources and for policy development regarding such allocations. The GNSO coordinates the activity of the commercial gTLD registries and policy development in that area whereas the CCNSO holds similar responsibilities for the ccTLD registries. The Technical Liaison Group coordinates activities related to Internet Protocol research and development and works closely with the Internet Engineering Task Force (IETF), the main body involved in such work.

The controversies surrounding DNS

At the December 2003 World Summit on the Information Society (WSIS),[27] the UN under Secretary-General for Information and Communications, stated:

> *“Unlike the French Revolution, the Internet revolution has lots of liberty, some fraternity and no equality”*

While few people would question the evident success of the Internet in terms of its openness, reliability and technological achievements, many feel uncomfortable with the current governance system in general and ICANN in particular. The following issues are hereby highlighted:

Representation

Some critics of ICANN question the legitimacy of the organisation in conducting policy development in view of its poor representation of governments (except for the US government of course). Unlike inter-governmental organizations such as the International Telecommunication Union (ITU), which advocates a top-down and government-led policy development process, ICANN has always favoured a more bottom-up and community-led policy development approach. While it is undisputable that this system has contributed to the success and openness of the Internet today, it can also be argued that this very success, which has turned the Internet into a public infrastructure of global and strategic importance, now warrants the scrutiny of governments. There has been a lot of debate on whether the management of the DNS should be executed by or, in collaboration with, multi-stakeholder bodies like the ITU. To ICANN’s credit however, it did recognize the need for more government participation and Stuart Lynn, former CEO of ICANN, did call for a reform process[28] that would include such participation.

US-Centricity

Another key aspect of the DNS geopolitics is the association of ICANN with the US Department of Commerce (DoC). Through this association, ICANN is viewed as being, ultimately, accountable to the US Government. This perception does not reinforce ICANN’s status as a broad, open and participative international organization.[29] At the World Summit

[27] http://www.itu.int/wsis/index.html

[28] http://www.icann.org/en/general/lynn-reform-proposal-24feb02.htm

[29] Geoff Huston, APNIC, The Internet Protocol Journal – Volume 8, No. 1, March 2005.

on the Information Society (WSIS) meetings, criticisms against this US-centricity of the current Internet Governance system has been voiced out by various interest groups, especially those from the developing world. This Uscentricity has also given rise to the widespread perception that any attempt by the international community to reform the Internet Governance process by introducing a more substantial role for governmental participation will be utterly resisted by the US. Thus, Houlin Zhao, Director of ITUT, in his paper[30] on "ITU-T and ICANN Reform", finds it necessary to reassure the US community that an ITU process will preserve the interests of the US government.

Resource Exhaustion

In its original conception, the ubiquitous IP address was designed as a 32-bit data structure and is referred as IPV4. The founders never imagined, even in their wildest dreams, that the Internet might, one day, exhaust the 2^{32} or 4,294,967,296 hosts![31] Thus, as IANA allocates the last remaining pools of IP address space to the Regional Registries, the International community suddenly realises how valuable this resource has become and the commanding position it will give those who will hold the last reserve of free IPV4 address space on earth. Hence, there is now an ongoing debate regarding the allocation policies that IANA should adopt for the remaining address pool. At one end of the spectrum of the debate, we have those who maintain that allocation should continue on a "need-to-use" basis whereas, at the other end, we have those who maintain that we should pre-allocate to regions or countries in anticipation of future developments. The latter view is popular among developing countries, which resents the fact that the US has had the "lion share" of IPV4 resources already since Internet development took off first in the North America region and with regions like Africa and Latin America catching up quite late. Perhaps, not surprisingly, the ITU has been proposing a country-based allocation policy[32] instead for the new IPV6 address space as an alternative to ICANN's allocation policy.

Dispute Resolution

Another problematic area fuelling the DNS polemic is the issue of dispute resolution. The current processes provided by ICANN for resolving name disputes (relating to identity, trademarks, copyright etc.) is embodied in its Uniform Domain-Name Dispute Resolution Policy or UDRP.[33] From the UDRP has emerged an entire form of jurisprudence that transcends the authority of local or even international courts of justice. In countries where the rule of law leaves something to be desired, it can be argued that ICANN act as a bulwark guaranteeing the right of individuals against totalitarian states. But, by the same token, critics also question the moral authority of ICANN over the state's sovereignty.

Conclusion

The DNS remains a controversial subject even after reforms carried out at ICANN and the involvement of governments and inter-governmental organizations like the ITU. The reason is because it touches the very heart of the Internet. It can be argued that Identity Management will provide a new thrust to the controversies and debates unless a global solution is found regarding Internet Governance. As nations and individuals places increasingly sensitive data online, it is expected that they will request more control over it.

[30] Houlin Zhao, Director, TSB, ITU, "ITU-T and ICANN Reform", 17th April 2002.

[31] http://www.potaroo.net/tools/ipv4/index.html

[32] Houlin Zhao, Director, ITU-T, ITU, ITU and Internet Governance, November 2004.

[33] http://www.icann.org/en/udrp/udrp.htm

Charles Raab: Questions and Points about a Regulatory Framework for Identity Management

1. Is ‘identity’ a sufficiently clear and uncontested concept around which to build schemes of management and a regulatory framework for them?

2. What are the implications of ‘identity management’ (IDM; serving the interests of database owners), as contrasted with ‘identity assurance’ (consumer-led) (See Crosby Report, 2008), for the relationship between organisations and individuals? Is this a false dichotomy?

3. Have controversies surrounding the Government’s ID Card Scheme contaminated the policy space for developing alternatives that would better elicit public trust?

4. The Data Protection Act 1998, and its Principles, are necessary but insufficient to regulate ID schemes.

5. They should be supplemented by more specific principles and guidelines for organisations seeking verification of identity, perhaps derived from the ‘7 Laws of Identity’ (Kim Cameron, Microsoft). Among these would be:

- Perform a privacy impact assessment before setting up an ID scheme
- Don’t identify if all you need is establishment of entitlement
- Follow the rule of data minimisation in terms of collection and retention
- Build in robust consent (and revocation) procedures
- Have strong access control and keep access logs
- Do not create a centralised database if possible
- Let people manage their own ID data, accessed by organisation when needed
- Help people to understand ID and privacy issue and choices
- [etc.?]

6. Should the safeguards designed into ID technology be mandated and/or incorporated into procurement rules?

7. Who should be in charge of the ID regulatory framework in the UK? What relationship would be desirable between the Office of the Information Commissioner and the National Identity Scheme Commissioner? Should the latter have greater regulatory custodianship?

8. Who should be responsible for citizen education and consultation about ID schemes, and how/when should these be done?

9. How far is (new) legislation needed for the regulatory framework? Would a special Code of Practice be necessary and sufficient, incorporating the supplementary principles?

10. Would international (e.g., EU and/or beyond) regulation be necessary for international transfers? What standards should be developed, and how?

11. How could industry groups, civil liberty/privacy and consumer NGOs, academia and others play a part in shaping and monitoring ID regulation, and in sustaining further development?

12. To what extent can lessons be learnt – and are they? – from other countries (and, for England and Wales: from Scottish developments) concerning ID systems and their regulation?

Chris Swan: Will credentials[34]

I'm going to be dealing with the final taboo, I hope that doesn't make you uncomfortable.

The question at hand is what happens to our digital assets when we die, and how do we deal with the identity management issues intertwined with this?

So far it seems that this hasn't been a problem large enough to deserve legislative and policy attention, but I suspect that's a result of demographics. Old people don't use as many online services as younger digital natives; but that's changing as online services become more ubiquitous and grannies sign up for social networking utilities so that they can see photos of their family. It's also a problem that will get worse over time; none of us is getting any younger, and the variety and usage of online services grows each day.

For services anchored in the real world like banking and utilities it would seem that the normal rules apply; accounts get closed down, or transferred, as appropriate. But even here there are issues, as online statements and billing remove the paper trail. If I have an online only deposit account then who even knows apart from me, the holding institution and the taxman?

Pure virtual services are clearly more problematic. If my contact book is in the cloud then who gets invited to the wake (and do digital Dunbar numbers mean a much bigger catering order)? If my photos are online how do they get passed on to my kids? Can my MMORPG artefact weapon be handed down from virtual father to virtual son (or at least can my crew keep my inventory)? This should be taken care of by the EULA or service agreement. I checked a few and found nothing. In most cases we have precious few rights even when we're alive and kicking, so it's no surprise that there's no provision for when we're dead. Maybe Richard Stallman is right to caution that we should all keep local copies of our data.

So what should be happening? Here are a few ideas:

- Service registries - a place where the online services used by an individual can be gathered together.
- Escrow credentials - so that next of kin (or executors) can access services on behalf of the deceased.
- 'Last post' provisions - for that final (micro)blog post, email or whatever to say goodbye.
- EULAs and service agreements with transferable rights.

Perhaps all of these things could be brought together into one service, a sort of digital undertaker. The link to identity is however key. As our needs for stronger proofing and tokens become more widespread the problem of identity inheritance (or in some cases identity delegation) become less abstract and less tractable. These things could also become features of emerging federated identity services, but in that case what would be the regulatory framework, and how do we deal with crossing jurisdictional boundaries?

[34] http://thestateofme.wordpress.com/2009/03/27/will-credentials/

Paul Trevithick

- Limits to liability. A perception that Identity Providers (IdPs) are liable for the actions of users and relying parties wielding and/or consuming the IdP's issued digital identities in the event that the identity information is incorrect (e.g. The wielder is a pretending to be someone else). The consequence is a reluctance to create IdP businesses.
- Data handling policy expression. Newer IDM technologies employ a local, smart client called a selector that could work to both protect the user's privacy. If the user could express their policy preferences and the counter party (e.g. a website with which the user is interacting) could express their actual policies in a machine-understandable manner, the selector could help the user engage in interactions with acceptable data handling policies and protect them from those whose data handling policies are unacceptable to the user.
- If a local copy of their own self-asserted identity data is created, does the user own it? When a user directly and explicitly enters identity information about themselves into an external system it is possible for an IDM system to automatically create a copy of these data. With the exception of special circumstances (e.g. work for hire), it would seem reasonable that the user owns these data. If this policy was clear IDM systems would be free to use these data on the user's behalf to avoid form-filling and other tedious forms of data entry into yet other systems.
- Are there inalienable rights to self-asserted identity data? When a user directly and explicitly enters identity information about themselves into an external system the assumption is that the legal owners of that system now own their copy of the user's data and are only limited as to what they can do with these data as part of a regulatory frameworks and voluntary privacy policies. But does the user have some inalienable rights with respect to these data? (e.g. the right to delete their profile data from a system (as well as all archives)). If so then IDM systems could be designed to help enforce these rights.
- Limiting identifiability. Although this fact isn't clear to policy makers or potential IDM systems implementers IDM doesn't necessarily imply increased identifiability and its attendant reduction in privacy. By moving away from a focus on identifiers and towards a claims-based approach, and by exploring the use of "one-way" mathematical functions (e.g. hashes) many interactions can be executed without revealing personally identifying information. Security need not be at the expense of privacy in all cases.

Philip Virgo: A Policy and Legal Framework for Identity Management

My objective from attending this workshop is to explore the validity of a few deceptively simple hypotheses and their implications:

1. That ID management disciplines date back to Ancient Sumeria (supposed roots of the notary/scrivener traditions) and transitioned to the electronic world over 150 years ago (authentication routines for East India Company cables, i.e. before the Indian Mutiny)

2. that tensions between the approaches to Identity Management of governments (to support taxation and military service and control dissent) and of business (to support transactions between those who have never met) go back nearly as far: with sporadic eruptions of extreme brutality on both sides e.g. the botched looting of the correspondence banking systems of the Knights Templar by Philip 1V and the urban revolt that destroyed the feudal structures of the Duchy of Burgundy. Attempts to seize banking records or destroy taxation or conscription records occur regularly through the ages. Today we have a plethora of attempts to introduce comprehensive integrated, federated and/or inter-operable by a variety of players with a variety of motivations, few

of which involve genuine choice or consent on the part of the “data subject”: alias customer, citizen, victim, patient. “client” or “miscreant”.

3. That alongside the experiences of governments in trying to keep electronic track of their “subjects” (for reasons ranging from taxation and law enforcement to education, heath and welfare) there is over 25 years of private sector experience with running ID management systems in digital environments, including in industries like security printing (e.g. De La Rue or Williams Lea), credit reference (e.g. Experian, Equifax), age cards and loyalty schemes (e.g. Citzencard, Nectar), payment clearing and correspondence banking (e.g. Vocallink and Identrust), Notaries (e.g. Metanoya/Global Trust Centre), the mobile operators (e.g. Vodafone) and, of course, direct marketing: in all its forms: now including the Internet.

4. that central to the sustainability, not just acceptability but whether they deliver their objectives over time, of ID management systems are the five R's:

   1. Responsibility (including ownership and the duties of "agents" for the "owner"),

   2. Registration (including marrying biography and biometrics to electronic credentials)

   3. Repair (when the registration and or credentials have been compromised)

   4. Revocation (either full because of serious compromise or partial, e.g. moved from "good citizen" to "suspected fraudster" or "convicted criminal")

   5. Redress (who should bear the cost of repair and of compensating the victims in the event of compromise - whether deliberate or accidental).

If those messages are correct (and I do mean *if* - I do not believe they are “self evident truths”). My interest is in:

- how the five Rs and the people processes that support them are addressed (or not) by the various ID management routines already operational or proposed

- the roles of professional bodies, trade associations, politicians, regulators etc. in identifying and encouraging good practice

- the means of assessing whether the supporting technologies on offer are fit for purpose and used correctly

- inter-operability between different types of scheme (legal basis, management structure, application, ownership etc.), including internationally, across jurisdictions, not just between similar schemes using different technologies

My day job is to help “educate” politicians and I wish to see them explore “least dangerous”, rather than “optimum” ways forward. I seek to delete the “o” when whenever I see it. In the “real” world “optimum” is almost always “seriously sub-optimum” before it is operational.

ANNEX IV: List of Attendees

John Borking
Stefan Brands
Chris Brown
Jacques Bus
David Chadwick
Neil Clowes
Piotr Cofta
Malcolm Crompton
Anna Dopatka
Bill Dutton
Joan Dzenowagis
Kaliya Hamlin
John Harrison
Iain Henderson
Ronald Leenes
David Lello
Karl Levitt
Jan-Martin Lowendahl
Lucy Lynch
Desiree Miloshevic
Anthony Nadalin
Vicki Nash
Gregory Neven
Vivega Padayatchy
Charles D. Raab
Marc Rotenberg
Mary Rundle
Mike Surridge
Chris Swan
Paul Trevithick
Dirk Van Rooy
Robin Wilton