A taxonomy of government approaches towards online identity management

Philip Seltsikas
Faculty of Economics and Business
University of Sydney

Hans van der Heijden
School of Management
University of Surrey

Abstract—A government’s approach towards establishing the online identity of its citizens is often subject to heated debate. This debate is sometimes obscured by the lack of clarity regarding the specific approach that a government adopts towards identity management. We propose a taxonomy for the type of identity management that a government can pursue. Our taxonomy identifies three essential approaches: a decentralized, a federal, and a centralized type. We illustrate our taxonomy using three countries that have approaches characteristic of each type: Australia, the United States, and the Netherlands respectively.

I. INTRODUCTION

Many government agencies around the world have begun to implement online versions of the services that they provide to their citizens. Examples of these services include the ability to file tax returns online, and the ability to claim benefits online. For each of these services, the government agency has a need to establish the identity of the individual requesting the service. How these identities are established, and the extent to which government agencies work together to do so, is the domain of online identity management.

Online identity management and identity management in general is subject to heated debate. This is particularly the case for those policy initiatives that attempt to share citizen data amongst several, seemingly unrelated, government services. Advocates of these initiatives claim that it will increase efficiency, prevent fraud, and help against terrorist activity. On the other hand, many have warned against the dangers of arriving at a “database state”, mentioning the erosion of civil liberties, the invasion of privacy, and the rise of a totalitarian regime or police state. Identity cards are often seen as the ultimate catalyst for these undesirable outcomes. Their (imminent) advent can prompt fierce political opposition (e.g., in the United Kingdom, as documented in [1]).

With the amount of public attention that identity management receives, it is easy to forget that information systems (IS) research can provide a meaningful contribution to the debate, and indeed, has been doing so for many years. For example, IS researchers have studied the concerns for privacy extensively, and have found that people’s stated concerns for privacy rarely correspond with their overt behavior online [2]. There are also more technical expose’s of how common digital identities can be established without having to resort to Big-Brother style databases [3]. A final example of a valuable IS contribution is the thoughtful work of Clarke [4] on digital personas.

It is our intention in this paper to contribute to this debate by formulating a taxonomy of government approaches towards online identity management. Such a taxonomy would allow us to classify government initiatives based on the approach they encourage or discourage towards online identity management. This would be helpful for a number of reasons. First of all, it would clarify the public debate. Second, it would be possible to compare more meaningfully the activities of one government with the activities of another. Third, it would allow us to start theorizing about online identity management. We could, for example, start to identify which of these approaches are the more successful and under what circumstances.

We are not aware of any previous attempt to characterize the type of government approach towards identity management. There is, however, related work that provides different ways in which one can identify types of identity. Mont et al. [5] illustrate how one could conceptualize different ways (“views”) of identity, in that governments, companies, and other institutions have different but overlapping representations of identity. Otjacques et al. [6] have examined the identity management approaches of 25 European countries, but have focused on the format of the identifiers in each country.

The remainder of this paper is structured as follows.
We introduce the three types of online identity management approaches in the next section. We then identify several key indicators of each management approach that will allow us to ascertain whether a government adopts one approach or the other. We apply those indicators to three different countries to demonstrate how each of these countries adopts a different type of identity management. We hope that this illustrates the usefulness of the framework because it shows how difficult it is to compare the approaches in different countries where they adopt different types. This, in turn, we hope will help clarify and contribute to the debate.

II. CONCEPTUAL DEVELOPMENT

For the purposes of our classification, four concepts need to be introduced and more precisely defined. These concepts are outlined below. The definition of these concepts is in line with other work in this area [3], [5], [7].

Government agency: A more or less autonomous branch of government. Agencies of interest here provide online services to citizens, e.g., online tax returns, online benefit claims, online requests for student loans, and so on.

Identity stores: An identity store refers to the database where verified identities are captured for use in government services.

It is important to distinguish between physical and logical identity stores. Physical identity stores reside in a particular data centre at a particular geographic location. Logical identity stores may combine disparate physical stores and provide the virtual perception of one identity store. In this way, government can share identity stores without these identity stores having to reside in one single database at one single data centre.

Identity registration system: These systems are the subcomponents of the e-government services where identities are managed and maintained. They are often administered separately from the services, as they can be re-used and shared by more than one different service. In fact we shall see that the degree to which these registration management systems are shared within and between the government agencies is a key element of our taxonomy.

Identity credentials: Credentials are the evidence that an individual supplies to demonstrate rightful “ownership” of the identity [7]. Examples of credentials include pin codes, passports, proof of address, bank statement, and so on.

Depending on the type of service, the government may require a higher ‘level’ of credential. Such levels of assurance can be used to classify the types of credentials that are required for each system. A Level 1 system might not require any credential at all (e.g., a public website with government announcements). A level 4 system (e.g., a law enforcement database) must require substantial verification of credentials to establish the correct identity.

Figure 1 brings these four concepts together in a flowchart, describing the essential steps of the identity management process.

The process can be decomposed into four steps. The citizen first supplies his or her identity credentials to an identity management system (step 1). Based on these credentials, the identity management system then establishes (or rejects) the identity of this citizen, and stores this information in the identity store (step 2). Following this, the citizen can successfully use an online service (e.g., request a student loan or query a law enforcement database, step 3). The online service will check the citizen’s credentials using the identity store that was previously mentioned.

We are now in a position to outline three types of approaches towards online identity management. We have called them the decentralized approach, the federal approach, and the centralized approach.

1) Decentralized approach: With this approach, each government agency develops its own identity registration systems and accompanying policies to suit its own needs.
It maintains and manages its own identity stores. The identity credentials issued to a citizen will be unique to the agency. The citizen will find these credentials of no use for accessing other government services online.

One of the advantages of the decentralized approach is that the impact of a security breach is potentially much lower than in any of the other approaches. This is because if one identity store is compromised, it will have no effect on any of the other identity stores.

One of the disadvantages of the decentralized approach is its inefficiency. Many tasks around the handling of identity are duplicated, and this can lead to inconsistencies and errors. Second, because identities are only known and verified at the local level, this approach creates opportunities for criminal activity. Finally, with this approach it has been argued that the government does not have a complete picture of the citizen. Such a complete picture would help a government to detect criminal patterns or terrorist activity.

2) Federal approach: Under this approach, a group of government agencies enter into a trust federation and agree using shared policy and technology standards and protocols to accept each others identity credentials to allow citizens to access each others online services.

It is important to recognize that such a trust federation could also be established between a government agency and a non-governmental organization, such as a bank. In the United States for example, such organizations are called credential service providers or trusted third parties.

On the face of it, this approach would seem to have the same advantages and disadvantages of the decentralized approach. There is a reduced impact of a security breach, but there is still duplication of work. The biggest difference, of course, is for the citizen, who only needs to supply identity credentials once to use every service in the trust federation. In the decentralized approach, the citizen has to supply identity credentials for each and every government agency.

The point needs to be made here that although there is great benefit for the citizen in this model, it is not immediately obvious where the benefits are for the particular government agency. If anything, this approach carries an additional administrative and technical overhead with it, i.e., using the extra arrangements to deal with the identity stores of other agencies. From a technical point of view, however, such overhead can be minimal, and commercial off-the-shelf applications are available that can manage this overhead seamlessly.

3) Centralized approach: Under this approach, a central government agency manages and stores citizen identities in a single location (at least logically), and all government agencies are required to connect their online services to the central identity provider (or identity verification service). For the citizen, this approach carries the same advantages as the federal approach. Citizens only need to supply identity credentials once. They can then use their identity in all government agencies that have embraced the separate identity service.

For a government, the centralized approach also carries clear advantages. There is no duplication of work, at least in theory. There is a complete picture of the citizen, which helps reduce criminal opportunities, and aids in intelligence activities. The “big-picture” is also much simpler to grasp, with an identity provider being the centre in a hub-and-spoke-like arrangement. These are all bona-fide arguments for a centralized approach.

The approach, however, carries its own set of disadvantages too. Because every citizen’s identity is stored in one place (at least logically), the impact of a security breach can be high. There are potentially great threats to privacy in case such a security breach does happen. Several high-profile cases in which much citizen data was lost illustrate that the occurrence of a security breach is not at all improbable.

Second, there is the possibility of misguided, inadvertent, or unintentional use of a citizen’s data by government agencies. There may be strict government guidelines as to which agency can use which part of the identity store for which reasons. Yet when those guidelines are not strictly followed, very undesirable outcomes may arise as a result.

Third, there are the technical challenges that need to be overcome to build such huge identity stores. Many governments do not have a spotless track record on the delivery of information systems within time and budget. Indeed, many citizens mistrust a government’s ability to create, develop and maintain such a huge identity store appropriately.

These are the three approaches to online identity management. A visual summary of each approach is provided in Figure 2.

III. CASE STUDIES

In this section we will look at three countries and examine their identity management type using our previously discussed framework. We have chosen these countries for illustrative purposes because they each represent a different approach in our taxonomy. They are Australia (decentralized approach), the United States...
Fig. 2. A taxonomy of government approaches towards online identity management
The data for these case studies was collected by the first author in the context of the project GUIDE, a European Union-funded project that investigated the potential for cross-border identity management within the E.U. In addition, secondary data was collected more recently and specifically for this paper.

**Australia**

Identity Management for Australian government agencies and departmental online services is the individual responsibility of each government owner of an online application. The general approach may be characterized as ad-hoc. Citizens wishing to enroll to use an electronic government service will in most cases have had to present a number of paper-based documents to each agency in order to provide the agency with verifiable data. The Australian Federal Government (Department of Defense) publishes an Information and Communications Technology Security Manual to provide guidance to agencies on a range of security issues including identification and authentication. Furthermore, the Australian Government Information Management Office (AGIMO) also publishes guidance to agencies on developing the processes and technology required to provide the desired levels of identity and risk management confidence (National eAuthentication Framework or NeAF).

Each agency or government department is responsible for establishing its own identity management system to support its own online government applications. Australian legislation governs aspects of this such as data protection for personal data that may be stored, but there is no mandated government-wide approach.

Agencies that adopt the guidance provided by AGIMO will consider five levels of assurance (0-4) that are defined in the NeAF. The levels (that are similar to those in our other two cases below) are based on the likely impacts of getting e-Authentication wrong by evaluating the nature of threats, the associated risks (e.g., financial loss) and their likely threat impact vis-à-vis the probability of their occurrence. This probability is increased or reduced by taking into account risk mitigation factors other than e-Authentication.

The NeAF assurance levels are defined as:

- **Level 0**: Null (insignificant threat impact)
- **Level 1**: Minimal (minor threat impact)
- **Level 2**: Moderate (major threat impact)
- **Level 3**: High (catastrophic threat impact)

In order to use an online government service, citizens register with each service independently and hence need to remember multiple pins, passwords, secret questions and the like. Some government departments have entered into bi-lateral relationships to share identity data for the purposes of cross-checking credentials to help counter identity fraud. With a decentralized approach to identity management it is difficult to ascertain the level of adoption as this type of information is not publicly available.

The Australian approach to identification and authentication is characteristic of our decentralized type. There are multiple fragmented identity services, some of which share information. In most cases, users of online government services can opt to register and use the service or they can transact with government using traditional paper-based means.

**United States**

In 2001, U.S. President Bush’s management agenda included mandates to increase the use of electronic government. This was to be operationalized through the Federal government’s 25 Quicksilver initiatives. These e-Government projects included government to citizen, government to business and government to government online services as well as internal efficiency focused projects. The linchpin initiative e-authentication was set up as a cross-cutting measure to facilitate the online verification of users of government services - and essentially to enable the remaining 24 quicksilver initiatives.

The US General Services Administration (GSA) set up the E-Authentication Program Management Office (PMO) in 2001. Following extensive research and consultation, in 2003 they had decided to adopt a federated identity approach and in 2004 created a technical architecture to support this. After several years of operation, the E-Authentication Federation was moved (in 2007) to a GSA line of business. It is now located in the Office of Integrated Technology Services of the U.S. Federal Acquisition Service. The management of the identity federation is split into Oversight & Policy and Operations.

The federation is predicated on a risk and assurance framework which consists of assurance levels. These were provided by the Executive Office of the President and describe an agency’s degree of certainty that the user has presented an identifier (or credential) that refers to their identity [8]; they are:

- **Level 1**: Little or no confidence in the asserted identity’s validity.
Level 2 Some confidence in the asserted identity’s validity.
Level 3 High confidence in the asserted identity’s validity.
Level 4 Very high confidence in the asserted identity’s validity.

Citizens, federal employees, or businesses who want access to an online government service go to the online application and are presented with a list of credential services that are appropriate for the assurance level required for the government service. The user then selects the credential service that has issued them a credential (for example their own bank). The credential service provider (CSP) asks the user for their credential and verifies it. The CSP authenticates the user to the government service and the user is given access. For level 3 or 4 transactions, a digital certificate may be used as a more secure credential (provided by the user to the government service and verified by a validation authority).

By 2009, 27 government agencies were using the federation services of E-Authentication to provide online access to their applications. Credential Service Providers include for example, a US bank (Wells Fargo), and many US government departments such as the Department of Justice and the Government Printing Office.

The US E-Authentication federation is a defining example of our federal approach. The US government has set out in detail the way in which the systems can use authentication mechanisms though shared, federal identity management systems [9]. It should be noted that the federal approach is not an open identity marketplace, rather, it is based on a variety of policies and agreements between all parties or members of the identity federation. In the US example, these agreements include the E-Authentication Federation Governance (a document intended to improve the internal management of the Federal Government), the E-Authentication Federation Operational Standards (a document that defines operational standards for Federation Members), and the E-Authentication Federation Relying Party Agreement (a signed agreement between the E-Authentication Program Management Office and the Relying Party).

The Netherlands

In 2003, four large government agencies founded DigiD, a shared online identity registration service for the e-government services that they are providing. The government agencies were the Social Insurance Institute (SVB, Sociale Verzekeringsbank), the Centre for Work and Income (CWI, Centrum voor Werk en Inkomen), the Employees’ Insurance and Benefits Office (UWV, Uitvoeringsinstituut Werknemersverzekeringen) and the Tax Authorities (Belastingdienst).

In early 2006 the systems and its operations were handed over to a common maintenance organization, GBO.Overheid. The organization forms part of the Ministry of Internal Affairs. As of today there are over 400 Dutch local authorities (towns and villages) who use DigiD as their central identity registration system.

The DigiD initiative carries three levels of assurance (similar to the four levels of assurance in use in the U.S. and Australia). Each level of assurance requires a progressively stronger set of identity credentials [10]. They are listed below:

- **Basis (basic)** Login name and password
- **Midden (medium)** Login name, password, and verification code supplied as text message
- **Hoog (high)** Identity card

Citizens can sign up for their identity at the website www.digid.nl. The identity is linked with the citizen’s Dutch identification number, the use of which is strictly prohibited by law and only permitted for use in public services. The online identity expires after 18 months of inactivity. Every time a citizen uses their DigiD identity it becomes valid for a further 18 months. The high level of assurance is not operational at the time of writing; identity cards have not yet been issued in the Netherlands.

The DigiD registration system enjoys widespread acceptance due to active promotion and endorsement by the Dutch tax authorities. One million users were registered in April 2006 [11].

The Dutch situation exhibits all the hallmarks of a centralized identity management approach. There is only one identity service, which is used by many different government agencies. It is of interest to note that the use of DigiD by government agencies is voluntary. Any government agency or local authority can join if it is permitted by law to use the Dutch identification number and provides some form of public e-service [11].

IV. Discussion

In this paper we have set out to ascertain types of government approaches towards online identity management. We have identified three types: the decentralized model, the federal model, and the centralized model. We have discussed several aspects of each model, and applied the taxonomy to three cases to illustrate its usefulness.
In this section we propose several extensions and development areas for the model. We look at the potential for harmonization of online identity management, whether we can frame the model as a maturity model, and the possibilities for further theorizing on identity management.

Harmonization of online identity management

An important question that can be asked in the context of identity management is whether identity management approaches can be harmonized across different countries. The natural domain where such a question arises is within the European Union (EU), where identity harmonization is of interest because it supports movement of people within the EU [12].

If EU harmonization of identity management approaches is ever to happen, it will certainly have to come a long way from where it is at the time of writing. The picture today is that of many different approaches, even within certain countries. The survey of Otjacques et al. [6] is particularly illustrative of this. The number of personal attributes (e.g., gender, age, and so on) that is connected with a country’s main national identity number ranges from four (Lithuania) to 24 (Bulgaria and Cyprus). In some countries, the centralized form of online identity management is in fact illegal (e.g. Germany).

We could tentatively suggest that the way forward for cross-border online identity management would be to adopt the federal approach, with several types of trust federations arranged as a federation of federations (as has been proposed by the EU project GUIDE). Such an approach would also heavily depend on the willingness of the EU member states to participate in a shared provision of identity management. Research that was conducted by Seltsikas and Papas [13] revealed that the types of trans-national government information system that would be needed to provide pan-European identity services can involve hundreds or even thousands of stakeholders and that there are significant challenges in determining a workable set of requirements for such an information system.

Maturity of online identity management

The second question we can put up for discussion is whether these types of identity management form part of a larger, more all-encompassing maturity model. It is almost inevitable for many countries to start off with a decentralized approach. This duplication of work then leads on to one or more federated versions of online identity management. Finally such a federal form may eventually lead to the fully centralized model. It is tempting to view these stages as phases in the lifecycle of online identity management. Recent research conducted by Seltsikas in the U.S. suggests that as the drivers for implementing identity management systems change over-time there are impacts on the implementation approach which could move a government between types [14].

Maturity models have a long standing history in IS (see e.g., the Capability Maturity Model and Nolan’s phases of IS integration). From research on those maturity models we know that the concept of maturity should be approached with extreme caution. First, “more mature” may not necessarily mean “better”. Second, “mature” phases may have been formulated to suit a vested interest, such as providing a commercial incentive to buy more consultancy services. Finally, maturity phases carry with them the notion of inevitability, in the same way that humans inevitably age and mature.

We could tentatively suggest that the decentralized approach is normally a precursor to either the federal approach or the centralized approach. In that sense, the decentralized approach can be seen as the “least” mature of the three. It seems sensible to suggest that the centralized approach is one that a government could arrive at without passing through the federal approach, and that the federal approach is one that a government could arrive at if a centralized approach is not deemed to be possible or desirable. Such suggestions are speculative at this point, and further research would be required to propose anything in this area with more confidence.

Further theorizing on identity management

The nature of this work is exploratory in the sense that we have conceptualized types of identity management, but we have not yet theorized about these types. In attempting to outline a taxonomy for identity management, we realize that some of our conceptual choices are open to debate. For example, it is legitimate to question whether there are just three types of identity management, or whether these are just points on a wider continuum of approaches. Indeed it can be argued that there is not one dimension on which these approaches can be mapped but several.

It is probably difficult at this stage to posit a theory on the success of online identity management. At this moment our conceptual apparatus is too crude to provide such a theory. However, a next step might very well be the development of an initial theory. Such a theory
would use the types of our framework as antecedents (why the government adopts the type that it does) or consequences (why the type has the ramifications that it has). It might also expand on the effectiveness of each of the approaches. We could tentatively suggest that most governments will eventually settle on a federal approach because the decentralized approach is too inefficient and vulnerable to fraud and the centralized approach creates too many privacy concerns and is vulnerable to fall-out in the case of a single-point of failure.

We offer these intriguing suggestions to the reader in the hope they will be fruitful avenues for further discussion and research, and will eventually extend our understanding of the government approaches to online identity management.

REFERENCES


