OPENNESS IN LATIN AMERICA AND THE PROBLEM OF IDENTIFICATION

Aaron K. MARTIN, Carla BONINA
Information Systems and Innovation Group
Department of Management
London School of Economics and Political Science
Houghton Street, London WC2A 2AE
UK
a.k.martin@lse.ac.uk, c.m.bonina@lse.ac.uk

Sofía GOLDCHLUK
Instituto Superior de Altos Estudios
University of San Martin
Parana 145
Buenos Aires, 1017
Argentina
sgoldchluk@googlemail.com

ABSTRACT

In this article we argue that ICT4D researchers interested in exploring and promoting concepts related to ‘openness’ must also consider potential impediments or limits to openness, including ongoing attempts to control interactions and transactions within the digital economy by requiring people to identify themselves. This trend is occurring in an increasing number of ways and contexts and facilitates the surveillance of citizens. Based in the development context of Latin America, our aims are twofold: to address the possible downsides and risks of identity systems in enabling openness; and to advance towards practical suggestions on how to mitigate them. After introducing identity as a problem area, we position our arguments in the debates on open ICT4D, open government, and identity management. We then review the current state of identity systems throughout Latin America, noting a general interest in new identity schemes based on digital technologies. We argue that debates related to openness for development and open government either assume that the problem of citizen identification has been solved or that the issue is unproblematic. In contrast, we show that there is a growing perception globally amongst policy makers, development agencies, and other authorities for the increased identification of users in ICT-mediated contexts, such as over mobile phone networks and on the Internet, as well as offline, which in turn complicates the objectives of openness and transparency. We end the article by offering tentative and provocative policy suggestions on possible ways to design identity management systems in Latin America in such a way as to enable openness and participation whilst mitigating possible negative social, political, and cultural effects.

Keywords: openness, ICT4D, identity management, surveillance, e-government, open government, Latin America, U-Prove, psychic ID

INTRODUCTION

New information and communication technologies (ICTs) promise an era of remarkable changes for developing countries, particularly in terms of how they can open new channels of connectivity and organization amongst individuals, civil society groups, businesses, and governments. In this process of change, these new technologies can also play an essential role in enabling new forms of transparency and accountability.

We repeatedly hear reports on the positive roles that technologies including mobile phones and social media are playing in organizing the masses, mobilizing groups to effect positive change, exposing misdeeds, shedding light on abuses of power, and holding wrongdoers to account. For example, the large protests that followed the disputed presidential elections in Iran in 2009 were organized with the help of ICTs, with the events being described as a "Twitter revolution" in the country. At the time this even led British Prime Minister Gordon Brown to comment that the Rwandan genocide would not have happened in a Twitter-enabled world (Viner, 2009).

However, achieving the goals of transparency and openness, as well as collaboration and participation, requires far more than using new technology. Harnessing the power afforded by ICTs, and particularly mobile telephony and the more recent web applications such as social networking tools, to generate positive impacts, will require additional infrastructure development. These complex infrastructures do not yet exist in most countries.

This paper confronts these issues head on. Based in the development context of Latin America, the aim of this paper is twofold: to address the possible downsides and risks of identity infrastructures in enabling openness; and to advance towards practical suggestions on how to mitigate them. While we understand that Latin America is a very heterogeneous region, there are some important general trends, including region-wide interest in new identity infrastructures, which allow us to make some generalizations. The paper begins by exploring some of the emerging problems related to identity in the information society, after which we position our arguments in the debates on open information communication and technology for development (ICT4D), open government, and digital identity management. We then review the current state of identity systems throughout Latin America, noting a growing interest in new identity systems based on digital technologies such as "smart" electronic ID cards (for online authentication), radio frequency identification, and biometrics. After exploring the case of Argentina, we argue that the debates related to openness for development and open government tend to either assume that the problem of citizen identification has been solved or that the issue is unproblematic. In contrast, we show how global trends indicate a growing perception amongst policy makers, development agencies, and other authorities in favour of the increased identification of users in ICT-mediated contexts (i.e., digital ID management), such as over mobile phone networks and on the Internet. We end with some tentative practical suggestions, intended to provoke, on possible ways to design identity management systems in Latin America to enable openness and participation whilst mitigating possible negative social, political, and cultural effects.

IDENTITY AS A PROBLEM

With the advent of the Internet and widespread take up of various ICTs in the last couple decades, the issues of identity and identification have taken on a newfound importance. Recent events speak to certain political realities that indicate that governments are unwilling to allow citizens to participate and organize fully online without some level of assurance about who is accessing certain data or services, or saying what to whom. For instance, South Korea recently changed its laws to require users to provide their real name and national ID card number before posting videos or comments on most websites, including popular social networking sites such as YouTube (Gonsalves, 2009). Turkey is also moving in this direction, with proposals to provide e-mail accounts and mobile phone numbers to its citizens which are linked to their national ID card numbers (Morozov, 2009). Likewise, national governments across the globe are developing and implementing Subscriber Identity Module (SIM) card registration policies, which require users to register their identity details when they purchase SIM cards, effectively eliminating anonymous communications in many areas. Whilst these registration policies are intended to help track down criminals who use mobile phones to commit crimes, as well as helping to reduce mobile phone theft, they simultaneously infringe on citizens' civil liberties.

The Obama Administration in the United States has also pointed to the importance of identity management in its cyberspace policies, noting that "[t]he [US] Federal government—in collaboration with industry and the civil liberties and privacy communities—should build a cybersecurity-based identity management vision and strategy for the Nation that considers an array of approaches, including privacy-enhancing technologies" (United States Executive Office of the President, 2009a, p. 33). As governments grapple to regulate the Internet and mobile phones and the many transactions and interactions that take place online, these trends are likely to continue.

And it is not just governments that are erecting and enforcing such registration and identification policies. Websites such as Wikipedia, a beacon of openness, crowdsourcing, and user-generated content, are currently altering their policies by requiring users to log-in in order to edit certain articles, which has in turn resulted in the recent mass exodus of editors. Thus, the goal of increased identification may come at the cost of increased participation. Such developments introduce difficult questions about the prospects for freedom of expression and association and, thus, any discussion about 'openness for development' must entertain questions about identification, anonymity, and privacy online.

Identity has even been described as "the new money" (Crosby, 2008).

> "Many hundreds of years ago, coins and notes facilitated trade between parties who didn't necessarily know each other. People put their trust in money, and trade multiplied many times. Now the rapid growth in remote "transactions" (by post, on the telephone, and over the internet), and the advent of many more processes that specifically call for identity to be verified in the public or private sectors, are significantly increasing the need for individuals to be able to assert their identity." (p. 3)

As with the mint, people now perceive the need to control identity. In response, both developed and developing countries have shown interest in government-managed identity systems to enable public service delivery and citizen interaction and participation online (Whitley & Hosein, 2009). However, with these new identity systems comes the real potential for surveillance and discrimination (Lyon, 2009). Here we get a glimpse of the dark side of openness: governments believe they must collect, store, process, and share all sorts of personal information about citizens if they choose to engage in these ICT-enabled environments.

OPENNESS, OPEN ICT4D, AND OPEN GOVERNMENT

In this section we review the related concepts of openness, open ICT4D, and open government. We acknowledge that defining openness is not an easy task. Fully conceptualizing what openness means is a project well beyond the scope of this paper. Thus, we keep our focus on exploring basic definitions and summarizing the current debates and problem areas.

Openness and open ICT4D

The academic and policy discussions around the concept of openness almost invariably point to a number of related social and technological trends that are resulting in a new set of opportunities for communication and collaboration. It is believed that the open structure and content of new ICTs represent a potential sea change in social structures, political activities, and opportunities for innovation (Smith & Elder, 2010; Heeks, 2010).

Proponents of the openness research agenda, including the IDRC and others (Hicks, 2010) point to the following trends as being indicative of a new order:

- The explosion and global diffusion of a new range of ICTs including mobile telephony and SMS, and the so-called Web 2.0 or social web, which permits increased interaction and collaboration amongst users.
- It is argued that from this technological infrastructure emerges "a new range of potential social and creative activities" (IDRC, 2008, p. 3). These include:
    - an increased capacity to co-ordinate, organize, and mobilize within networked societies
    - the harnessing of collective intelligence and new forms of peer production
    - the enormous growth of user-generated content; and
    - a new wave of user-driven innovation (IDRC, 2008, pp. 3-4).

In sum, openness is seen a new means of and opportunity for organizing social activities such that access to information, online participation, and collaboration are made universal, rather than remain restricted. Yet, what does all of this openness talk mean for developing countries? And, furthermore, how can ICT4D harness these concepts of openness to further the development cause?

Emerging from this general discussion on openness is a hypothesis related to open ICT4D which argues that these recently opened social and technological spaces, and their attendant participatory and collaborative dimensions, can bring with them real developmental benefits (IDRC, 2008; Smith & Elder, 2010). These benefits include, for example, improved education for people within developing countries, improved health outcomes, timely information regarding imminent natural disasters (such as approaching tsunamis or rising flood waters), enhanced government transparency, reduced government corruption, and so on. However, the open ICT4D hypothesis remains largely untested, primarily because of the newness of the technologies involved and their current low levels of penetration in developing contexts. We still do not know whether and how openness leads to development. There are also many infrastructural impediments to such developmental benefits which require critical evaluation.

Open government

In this section we focus on how arguments about openness apply to the area of e-government – known as open government. We focus on open government in particular because it will very likely require robust identity management systems for it to realize its full potential. Across the globe, most current and proposed identity management systems are government-sponsored, and so it is also relevant to explore the parallel developments of openness and identification from the perspective of government institutions. As discussed above, the concept of "openness" permeates several dimensions of society, and governments are no exception. Enabling and developing open government has also appeared as one key aspect in the discourses on ICT4D (IDRC, 2008; Heeks 2010).

Open government has been conceptualized in different ways, with various actors providing their own take on the issues. According to the Organisation for Economic Co-operation and Development (OECD), building open government helps to facilitate the core aspects of public sector reform; that is enabling a more responsive, efficient, effective, and participatory government (OECD, 2003, 2005a). In this context, the OECD states that open government covers three main elements (OECD, 2005b):

- Transparency, understood as exposing government institutions to public scrutiny;

- Accessibility of relevant and understandable information to anyone, anytime, and anywhere; and
- Responsiveness of government institutions to new ideas and demands.

The OECD refers to "openness" then as a concept that goes beyond the sole idea of transparency. From the public's perspective, they affirm, "an open government is one where business, civil society organisations and citizens can "know things" – obtain relevant and understandable information; "get things" – obtain services from and undertake transactions with the government; and "create things" – take part in decision-making processes" (OECD, 2005b, p.1).

From a slightly different angle, the recent open government initiative launched by the Obama Administration in the US further advances the openness debate. In early 2009, President Obama signed the memorandum on Transparency and Open Government in which he announced his administration's commitment to achieving an "unprecedented level of openness in Government" (United States Executive Office of the President, 2009b). The US open government initiative is designed around three core values:

- Transparency: to enable greater accountability, efficiency, and economic opportunity by making government data and operations more open;
- Participation: to create effective opportunities to drive greater and more diverse expertise into government decision making; to listen to public opinion and to increase opportunities for public engagement; and
- Collaboration: to generate new ideas for solving problems by fostering cooperation across government departments, across levels of government, and with the public.

The OECD and US approaches are similar although the latter goes one step further when describing the core elements of openness. Both transparency and accessibility, as depicted by the OECD, are understood in the US open government initiative under the notion of transparency. Both cases argue for making more information more readily available to the public, a process in which ICTs can play a major role. In addition, the

OECD call for responsiveness is also contemplated in the US case under the label of participation. The focus is not only on being more transparent to the public but also on listening to their demands. Whilst the two approaches are very similar, the US open government initiative takes one further step and adds an additional core value of collaboration.

Within this context, the use of new ICTs and the deployment of e-government are seen as the most promising tools in terms of achieving the goals of openness in government (OECD, 2005b). Yet, as mentioned earlier, the push for a more open government has not happened in a vacuum; the open government initiatives are part of a larger wave of public sector reforms initiated over two decades ago under the labels of ‘reinventing government’ and ‘new public management’ (NPM). Initially associated with public sector restructuring in the UK, New Zealand and Australia during the eighties, NPM practices spread across many western countries. NPM proposes a project of reforms to redefine managerial and governance practices in the public sector in line with objectives typical of market economics. Thus, NPM’s common features were downsizing, accountability, focus on performance, concern for results, decentralization and organizational disaggregation, and the “importation” of several private sector practices into public sector management (Borins, 1997; Gruening, 2001; Hood, 1991; Kettl, 2005). Within this reforms scenario, governments have invested large amounts of money in public information systems (e-government), aiming at enhancing efficiency and policy effectiveness as well as to achieve transparency and political participation (Bellamy & Taylor, 1998; Fountain, 2001; Gil-Garcia & Pardo, 2005; Gronlund & Horan, 2004; Heeks, 1999; Kamarck, 2007). The approaches that define e-government according to its stages of development (Layne & Lee, 2001; UN & APSA, 2002) are thus useful in illustrating the parallels between e-government and open government ideas. Even when some of the assumptions may differ, the e-government models that build upon stages of development depict three general maturity phases: the early, middle, and later stages. As the stages evolve, the levels of interaction with the citizen increase in complexity (Layne & Lee, 2001; UN & APSA, 2002). The early stages are usually more static and entail gathering and putting government information online (e.g., launching the first website). The middle stages include some forms of transactions, in which the government opens channels to communicate both ways with citizens. Putting databases online to support transactions and enabling e-mail communications are common examples of the middle stages. The more mature stages entail further organizational complexities, as more integration is required, not only with the citizen but also between government agencies (Layne & Lee, 2001; UN & APSA, 2002). Examples of the most mature e-government stages are the one-stop-shops in which citizens can comply with procedures online, through a single point of access.

Transparency, in the form of making government information publicly available to citizens, has been recognized as one of the core elements of many e-government strategies in their early stages. Latin American countries are no exception to this trend. For example, the Mexican legislation for access to information approved in 2001 includes a rule on record management in which agencies must put public information online[1]. This rule requires federal agencies to create official websites for information dissemination and it has become the main driver for the development of additional government agency websites in the country. In terms of political participation, there are several examples of the use of digital channels in Latin American governments (UN, 2008; West 2005, 2007). The case of Brazil and the House of Representatives e-participation website has been

[1] Mexican Federal Transparency and Access to Public Government Information Law, Article 9.

highlighted as a salient one (UN, 2008), but it is only one of the many examples of e-participation channels governments have launched in recent years.

But the potential benefits of openness do not stand alone without risks. Even though it is clear that transparency has many virtues and utility for political systems, there are potential harms as well, which are often ignored. In a recent essay, Lessig (2009) addresses the perils of openness in government. Alluding to what he calls the "naked transparency movement" in the US, Lessig illustrates how different circumstances may harm the good in transparency. He particularly refers to how the misuse of publicly available information may put the political system into crisis as there is a risk in revealing information, for the sake of transparency, that may not be accurate or may raise confusion or false accusations due to unexamined assumptions about causality.

Selecting the right technologies and appropriate channels to communicate with the public is not straightforward either. Collaborative technologies such as Web 2.0 provide attractive cost-effective solutions to facilitate participation, especially in the middle and later stages of e-government projects. However, the goal of transparency and openness as well as collaboration and participation requires far more than using the latest and newest technology. Taking advantage of the potential benefits of ICTs, and particularly the more recent applications such as social networking, to generate positive impacts will require additional infrastructure development; particularly infrastructures for citizen identification and authentication. Given the fact that governments have a unique relationship with citizens (e.g. voters and elected officials, tax payers and tax offices), electronic authentication policies present several issues, including privacy implications (Holden & Millett, 2005). The next sections discuss how identity management policies and technologies can both impede and facilitate open e-government, and open ICT4D more generally, depending on their configuration.

DIGITAL IDENTITY MANAGEMENT

The term identity management covers a wide range of policies and technologies which enable organizations to identify or authenticate users of a system or service. These organizations include bodies such as government departments responsible for issuing identity credentials to citizens (e.g., ID cards and passports), but also other organizations such as companies that need to assign certain access privileges to employees or other users (e.g., customers). Increasingly, these identity management systems are being deployed in online contexts where face-to-face interaction is difficult (if not impossible) because of the technological medium and where concerns about the reliability, motivations, and trustworthiness of users are growing. Digital identity management requires a different type of infrastructure and set of processes than offline, paper-based means of identification. If leveraged correctly, these identity systems can facilitate the technologies that underlie open ICT4D and open government. If they are poorly conceived and designed, such policies and systems can introduce new problems related to privacy, surveillance, and discrimination that could halt the openness movement before it gathers momentum.

We cannot fully capture the breadth and depth of issues and concerns related to digital identity management in this paper, for obvious reasons of scope and focus. Readers interested in a review of the issues should consult the literature (see, for example, Whitley & Hosein, 2009; Lyon, 2009; OECD, 2009). However, for the purposes of exploring appropriate identity management policies that promote the virtues of openness, we want to discuss the important distinction between identification and authentication, as well as the related concepts of pseudonymity and anonymity.

Identification and authentication

Identification is the process by which a person's identity is revealed (e.g., "this is Carlos Gardel", the famous tango musician). This is a different process from authentication, although in the common vernacular the two concepts are often conflated. Authentication involves the granting of access to something and does not necessarily require the revelation of an identity. For example, some typical authentication requests include:

- "Is this person a Uruguayan citizen?" (e.g., at a border crossing),
- "Is this young person at least 18 years old?" (e.g., when proving whether someone is of legal age to consume alcohol),
- "Is the person an inhabitant of Buenos Aires?" (e.g., when accessing a restricted local service).

At no point in these authentication requests does the person's identity (or components thereof – i.e., his or her name, ID number, or date of birth) need to be revealed. Authentication requests are therefore, fundamentally, yes/no type requests. Identification and authentication are thus distinct activities which need to be treated differently by systems that manage identity information. The over-identification of users, especially in contexts that in reality only require authentication, can lead to the creation of extensive data profiles about people's activities, preferences, and the like, triggering concerns about surveillance (Clarke 1994). In most scenarios, what is actually needed to complete a transaction or access a service is an authentication measure, and not full identification. In this context, then, it should be possible for users to provide pseudonyms or to remain anonymous in their dealings with organizations, as long as the right information is disclosed for the relevant transaction (e.g., whether the person claiming benefits is entitled to them). The use of pseudonyms and anonyms (that is, remaining anonymous) is particularly important online where, as the famous saying goes, "On the Internet, nobody knows you're a dog". Yet, how do we ensure that, the wrong people claim social benefits without creating an identity system that leads us to ‘sleepwalk into a surveillance society’? As was discussed above, there is a global trend toward the increased identification of users in a wide range of contexts and for ever more transactions, often when identification is overkill considering the types of transaction or interaction taking place. Many of these contexts implicate the technologies of Web 2.0 and social networking, which are at the heart of open development and open government initiatives.

Government-sponsored identity management systems

When governments do identity management, it is often to “solve” many different “problems” at once, including protecting citizens from the alleged risks of terrorism, fighting identity theft and administering social benefits (Lyon and Bennett, 2008). In the case of public service provision, and as discussed in the previous section, digital identity management could be a good enabler of e-government. This is particularly relevant in helping governments to facilitate the integration of services that are present in the mature stages of e-government deployment.

But identity management is also crucial in facilitating international mobility. The use of identity documents to facilitate travel is particularly relevant to our discussion because of the international standards that are required for identity cards and passports. These standards mandate the types of personal information to be collected and used in the issuing of documents. In certain contexts such as the UK, these standards have also been used as a means to justify the mass collection of large amounts of bibliographic and biometric data from citizens as part of their proposed identity system (Hosein, 2004). Once these masses of data are collected and stored in databases, there is an ineluctable tendency to use them regularly and for purposes that were originally not planned (i.e., so-called scope creep). The “database state” thus emerges as an area of concern (JRRT, 2009), whereby governments' use of ICTs and especially large databases is negatively viewed by people as intrusive and unwarranted.

NATIONAL IDENTITY SYSTEMS IN LATIN AMERICA

Many of the abovementioned issues and problems related to identity management apply to the Latin American context, where across the region there is a historical legacy of government-sponsored and administered identity card systems. These national ID systems have, for many years, required the enrollment and databasing of substantial amounts of personal information and, to date, have relied on the verification of identity documents in many face-to-face transactions, including domestic and trans-border travel. Appendix 1 lists the current state of national identity card schemes across Latin America, including details on the names of the identity card systems; their institutional sponsors; whether their databases are centralized; whether so-called smart cards are in use; what sorts of personal information are collected and used; what sorts of biometrics are involved (if any); how the cards are used; and any forthcoming planned "upgrades".

The general picture that emerges from the data is that these systems are inadequate for identity management in an information society, and particularly one inspired by the technologies that underpin open ICT4D and open government. Most of these systems are relics from the pre-digital age, and are based on paper or plastic documents. They rely on the extensive use of ID numbers in all facets of life, and if these practices are carried over into the online space, there will be negative consequences.

In the following sub-section we zoom in on one country in particular, Argentina, as an illustrative example of how ID cards and ID numbers are used in Latin America.[2] In most

[2] We do not intend to generalize our conclusions from the Argentinean case, but rather seek to highlight some of the issues that might be applicable to other countries.

countries these uses and misuses are taken for granted in day-to-day life and remain uncontroversial.

The DNI in Argentina: a case vignette

There are two IDs in Argentina: the DNI (Documento Nacional de Identidad), which has been issued by the ReNaPer (Registro Nacional de las Personas) since 1948, and the CI (Cédula de Identidad), which is issued by the police to every person without a criminal record. People can use these IDs interchangeably, except when they are voting or engaging in banking transactions, for which they can only show their DNI. Nowadays, when companies make promotional offers, they only accept the DNI as a valid proof of ID. Thus, the DNI is collected and processed by many different organizations; a state of affairs which has led to its overuse and occasional abuse (Thill, 2007). These days identity fraud using the DNI is a regular occurrence (Thill 2007).

Argentina is currently launching a new DNI. This will consist of two different documents: an improved version of the old DNI ("DNI libreta") and a new card ("DNI tarjeta"), containing all the information in the DNI. This card will be used for all the transactions that people currently use the DNI for, except for voting. This will also make the CI obsolete in the future. In the future there will be a single ID number being used for most identity verifications.

The new DNI tries to shorten delivery times from 30 to 5 working days. It also aims at creating better communications between the ReNaPer and the provincial civil registries when someone changes their address, when new voters are added to the voter registry, and when dead people are removed from the electoral list (One of the most common cases of ID fraud in Argentina involves people voting with dead people's DNIs (Sábato

2001). In order to do so, the government is opening new “fast documentation centers” (CDR – Centro de documentacion rápida) which will be set up all around the country.

These concerns reflect those explored by Murakami Wood and Firmino (2010) in the Brazil case, where the problem of identity fraud results from the insecurity of identification documents, the overuse of ID numbers, and the absence of strong data protection laws.

Argentina and Brazil, like many other Latin American countries, are in the very early stages of building new digital identity infrastructures. Mexico is also pursuing a new identity system, complete with fingerprints, iris biometric, and digital facial recognition. As these systems are developed, there are important questions to be asked regarding good design. In the next section we provide some policy suggestions on how best to design identity management systems such that they are suitable for the digital era and can support the aims of open ICT4D and open government.

FUTURE SCENARIOS AND OPPORTUNITIES FOR INNOVATIVE DIGITAL IDENTITY MANAGEMENT IN LATIN AMERICA

How can Latin American countries that are interested in investing in new identity systems build infrastructures that engender trust, protect privacy and limit the potential for citizen surveillance, whilst enabling a degree of openness for development? The solution is neither straightforward nor guaranteed; however in this section we offer a few policy recommendations on how to achieve ‘identity management for openness’. We do so fully aware of the limitations of policy recommendations and we stress that what follows is more than anything intended to stimulate creative reflection on the issues rather than serve as a strict “how-to” prescription. All solutions, no matter what the problem, are necessarily partial and incomplete, and it is essential to consider the particularities of the context at hand when implementing identity management policies and systems.

The recommendations come in two parts. The first set of recommendations builds on recent guidelines from the OECD concerning digital identity management, whilst the second part summarizes recent thinking on how to build innovative, privacy-friendly, user-empowering identity infrastructures based on digital technologies.

The OECD has recently published a policy document in which they provide useful guidelines and recommendations for digital ID management (OECD, 2009). Working with stakeholders to create favorable conditions for the development of digital ID infrastructures appears as the key goal as far as public policy design is concerned (OECD 2009). Such co-operation takes on a special significance when the design and implementation of identity management systems is undertaken by non-governmental actors. We will return to this point shortly. There are four main challenges to good digital identity management to take into consideration:

1. *Interoperability*. Ensuring compatibility across organizations and at the same time avoiding harm to innovation and flexibility is one of the major concerns raised by the OECD. Interoperability issues entail several dimensions: policy, legal, procedural, and technical. From a policy level, articulating a clear set of ID management policies remains the key challenge for organizations. Governments are also regulated by legal obligations, which may posit a burden in ensuring interoperability. The main issue from an international perspective would be to minimize regulatory complexity. At the procedural level, adopting digital ID management systems may require reviewing the work processes of each organization. From a technical point of view, the challenge appears in

encouraging the development of common standards without losing flexibility to innovate.

2. *Empowerment*. Education and awareness of new ID systems are key features for empowering users and building trust (p. 13). The main considerations range from security and privacy controls, to transparency in the enrollment processes and the clear attribution of responsibilities (i.e., who is accountable for what in the ID system).

3. *Ensuring security*. In this area, the major issues entail designing and implementing policies to protect identity data. Both reliable and robust ID management systems are crucial in this respect. Policies should be consistent in ensuring three aspects: availability and accuracy of identity information (e.g., identity data should be available when and where required); confidentiality, which entails minimizing any potential corruption of ID information (especially in the case of sensitive personal data); and integrity, which refers to minimizing the disruption of an ID management system (or any other ID system that may be dependent on it). Auditing controls and technology choices are central in the security of ID management systems.

4. *Ensuring privacy*. Both privacy and security controls are key in terms of ID management. As much of the information contained in ID management systems is personal information, how to protect identity information probably remains the most relevant question. The main issues the OECD identifies in this area are: (i) ensuring long–term storage and processing data on a digital format; (ii) facilitating anonymity and pseudonymity for the freedom of expression, which raises concerns regarding data protection; responsibilities and accountability propositions are complex in ensuring which data should be veiled and under

> which circumstances could be unveiled; (iii) it may not be clear which areas of ID management should definitely be regulated by governments and what identity practices could be left to market forces.

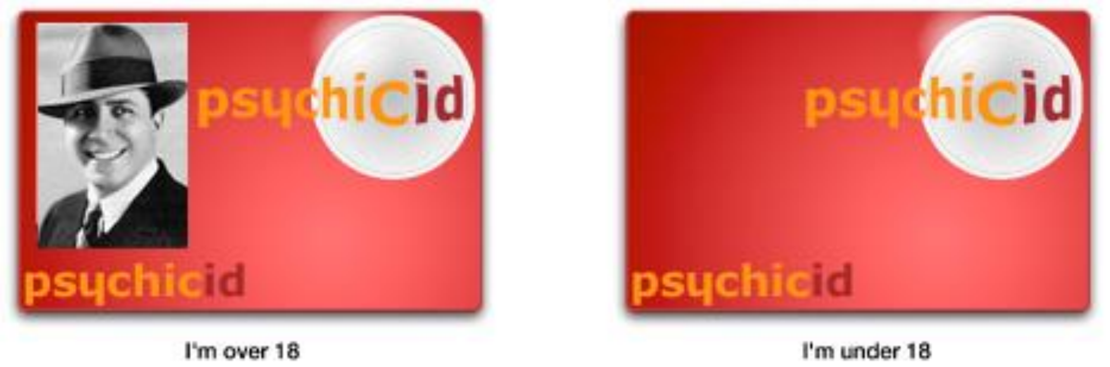
Innovating identity management

The four areas that the OECD identifies are useful and important although fairly broad and abstract. We can apply these broad ideas to a practical discussion on how to 'do' identity management for openness. Building on ideas developed by Brand (2000), Birch (2009) has provided some initial ideas for such a blueprint; his vision is for an identity system that achieves interoperability via smart cards or an already ubiquitous information technology: mobile phones; whilst simultaneously empowering users and ensuring data security and privacy. His proof of concept builds on the ideas of data minimization put forth by Crosby (2008) and permits the use of pseudonyms and anonyms, where appropriate.

Very basically, Birch's idea is to design an identity system whereby the only data disclosed during a transaction is that data which the subject wants to share. Importantly, data will not be divulged unless its recipient is entitled to see it. Inspired by the *Dr. Who* television series, Birch calls this proof of concept "psychic ID" (2009). In the television program, Dr. Who's "psychic paper" has special properties which induce whomever is inspecting the paper to see what the holder wishes them to see printed on it.

Birch's vision builds on this lesson from science fiction, to move away from the old ID card technologies that limit the possibilities for online interactions and user privacy. As we discussed above, most ID cards currently in circulation in Latin America do not easily permit online authentication and usually display lots of personal information of the face of the card by virtue of their historical legacies, which in turn introduces privacy concerns. In contrast, Birch's 'psychic ID' would only reveal the information necessary for the transaction. Let us illustrate how Birch's 'psychic ID' works by returning to our previous examples.

If at a nightclub the doorman, or bouncer, wants to verify that one is allowed to consume alcohol, he can send an authentication request to one's smart card or mobile phone (more on this later) and the response would be as follows:



I'm over 18

I'm under 18

Figure 1: What the bouncer sees (Adapted from Birch, 2009)

This plainly answers the bouncer's request as to whether one is old enough to enter the bar. Importantly, at no point during the interaction does the card holder reveal any unnecessary personally identifiable information (including even the card holder's date of birth), with the possible exception of the face image which is used simply to ensure that the card is with its rightful owner. Moving on to the second example, if at a border crossing a police officer wants to know if one is an Uruguayan citizen, s/he can send the appropriate request and, assuming s/he has the right to make such a request, s/he would receive one of the following responses.

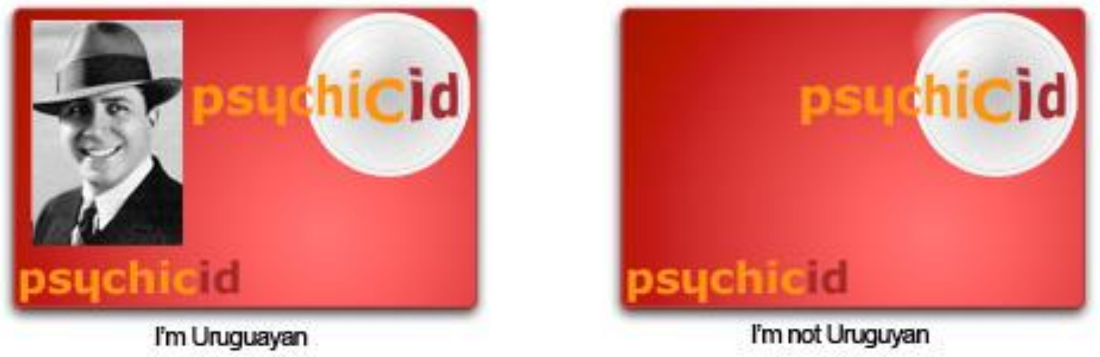


Figure 2: What the border agent sees (Adapted from Birch, 2009)

Likewise, with a restricted local service, such as health care, a receptionist at the local clinic could query one's smart card or mobile phone and receive one of the following responses, plainly communicating whether one is entitled access to the service.

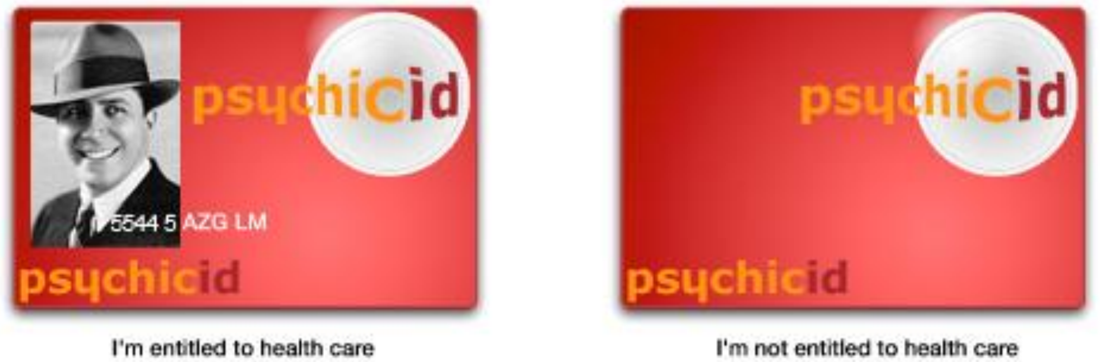


Figure 3: What the receptionist at the clinic sees (Adapted from Birch, 2009)

'Psychic ID' can also support virtual identities online, and thus lends support to many of the technologies such as Web 2.0 that underlie open ICT4D initiatives. For example, in an online, open government-type environment where one might want to remain anonymous or pseudonymous due to the political nature of the debate, but where the host of the debate also needs to ascertain whether you are entitled to debate (e.g., based on national citizenship or local residency), 'psychic ID' can be used in conjunction with one's computer and a personal identification number (PIN). This arrangement will release a pseudonymous identity and a placeholder picture without disclosing one's actual identity. Birch envisages ‘psychic ID’ cards permitting multiple identities, depending on the context.

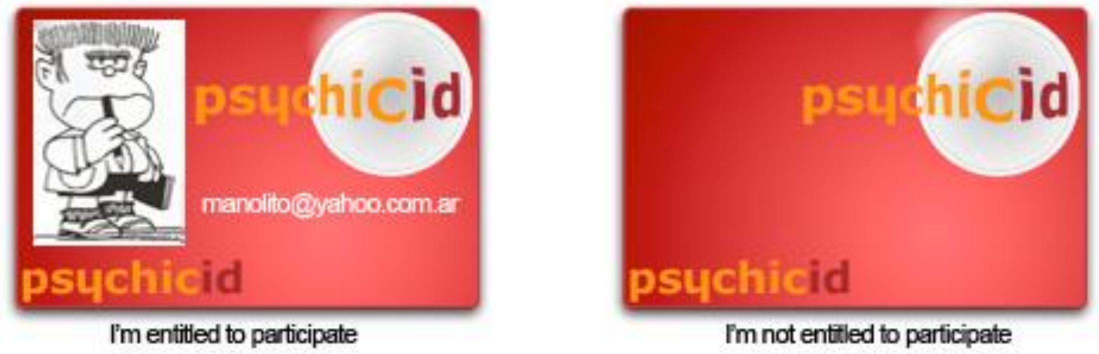


Figure 4: What the open-government debate host sees (Adapted from Birch, 2009)

What is especially fascinating about Birch’s proposal is that he envisages it working on both smart cards and mobile phones. “I claim that not only is it eminently practical but we already have the technology to build it.” (no page number)

Figure 5: Mobile phone-based psychic ID (Birch 2009)

The technology he has in mind is mobile phones, whose penetration rate has increased spectacularly in Latin America over the last 10 years (see Figure 5). The hardware and software running on the current and next generation of mobile phones is suitable to support the identity system Birch proposes, and importantly is something most people already have.[3]

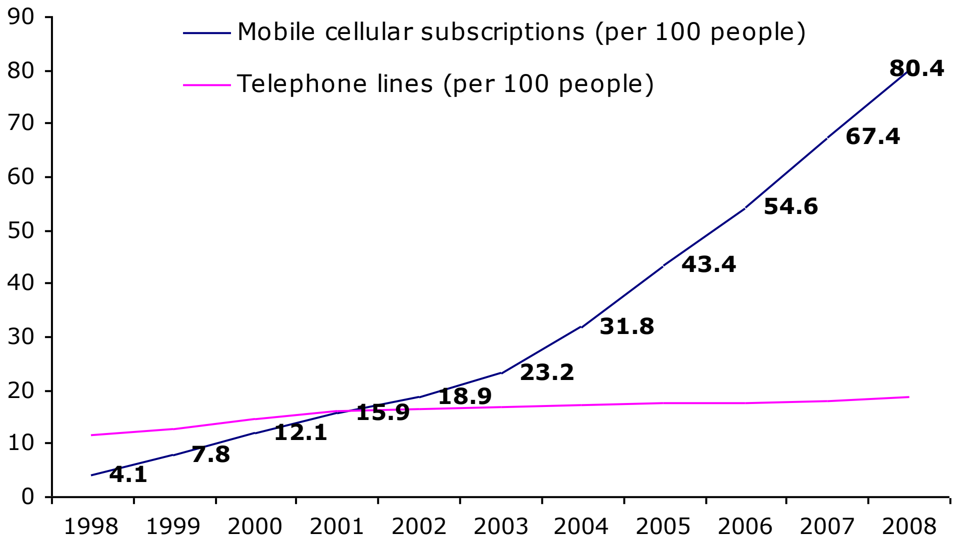


Figure 6: Mobile penetration in Latin America 1998-2008 (World Development Indicators, 2009)

Reinforcing the point, the fact that access to and use of mobile phones in the region has grown dramatically, makes Birch's proposals more attractive. This is particularly relevant considering that building and investing in technical infrastructures is usually a matter for economic and political debates. It is important, however, to highlight that there are certain economic and social realities in the Latin American context that complicate such proposals for innovative ID. For example, mobile phone theft is a major issue in many countries across the region. Thus, unless proper security protections are put into place, the use of mobile phones as part of new identity infrastructures might increase the potential harms of identity theft and privacy invasions.

[3] For Birch, all of this must happen with appropriate cryptography, which is a discussion we cannot enter here due to scope limitations. We encourage readers to see his paper (Birch 2009) or Brand's (2000) elaboration for further details.

Also, Birch's proposal also means that governments will likely take on a different role in the provision and management of identity information. Birch sees this new identity system as a utility and governments as regulators of that utility, and not necessarily providers. As utility regulators, governments would be responsible for upholding five principles:

- Universality: "The process for conducting an identity transaction should be exactly the same, regardless of the status of any individual"
- Symmetry: Anyone should be able to assert *and* verify another's 'psychic ID', but importantly card (or phone) holder must be able to hide certain credentials if they want for privacy's sake
- Speed: An identity system needs to be convenient and fast
- Practicality: A tamper-resistant identity token such as a smart card or mobile phone is considered a practical necessity
- Extensibility: As an infrastructure, Birch's identity system is something that anyone should be able to access and build on

We conclude this section with some further critical reflections on Birch's proposal and the limits of supporting open ICT4D with the infrastructures he envisions. First, it is a truism these days that privacy is a culturally relativistic phenomenon (for example, survey research shows that public understandings of privacy are very different in Asia than in North America (Lim et al, 2009), but it is important to consider whether Birch's privacy-enhancing approach to identity management 'translates' to the socio-cultural contexts of Latin America where the concept of privacy arguably means something different than in the UK context. This is an empirical matter, of course. Birch's approach also requires a transfer of authority from the government organizations that formerly issued identity credentials to a range of different actors. It remains to be seen whether this transfer of power is realistic in the Latin American context, although as we have already argued, the high levels of mobile phone penetration in the region make it a fitting context for such an infrastructure.

CONCLUSION

In this paper we have taken some initial steps toward critically evaluating the role of identification and authentication in open ICT4D, including open government. We have argued that programs that encourage and promote openness must simultaneously consider the identity infrastructures that enable such interactions and transactions. If appropriate infrastructures are not put into place, the shift towards these open spaces could result in widespread privacy invasions, surveillance, discrimination, or worse. Although there is no perfect way of designing and implementing new digital identity systems that both respect privacy and civil liberties and guarantee all the good of openness, here we have proposed certain areas worth exploring. In doing so, we aimed to help create the basis for further discussion on digital identity within the next generation of online access, participation, and collaboration.

BIBLIOGRAPHY

Bellamy, C., & Taylor, J. A. (1998). Governing in the information age. Buckingham; Bristol, PA, USA: Open University Press.

Birch, D. (2009). Psychic ID: A blueprint for a modern national identity scheme. Identity in the Information Society, 1(1).

Brand, S. (2000). Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy. MIT Press.

Borins, S. (1997). What the New Public Management is achieving: A survey of Commonwealth Experience. In L. Jones, K. Schedler & S. Wade (Eds.), Advances in International Comparative Public Management (pp. 49-70). Greenwich: JAI Press.

Clarke, R. (1994). The Digital Persona and its Application to Data Surveillance. The Information Society, 10(2). Archived at: http://www.rogerclarke.com/DV/DigPersona.html

Crosby, J. (2008). Challenges and opportunities in identity assurance. London, HM Treasury, 1-48.

Fountain, J. E. (2001). Building the virtual state: information technology and institutional change. Washington, D.C.: Brookings Institution Press.

Gil-Garcia, J. R., & Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. Government Information Quarterly, 22(2), 187-216.

Gonsalves, A. (2009, April 13). Google Scales Back YouTube Korea. InformationWeek. Archived at: http://www.informationweek.com/news/internet/google/showArticle.jhtml?articleID=216500489

Gronlund, A., & Horan, T. (2004). Introducing e-Gov: History, Definitions, and Issues. Communications of the AIS, 15, 713-729.

Gruening, G. (2001). Origins and Theoretical Basis of New Public Management. International Public Management Journal, 4(1), 1-25.

Heeks, R. (1999). Reinventing government in the information age. New York: Routledge.

Heeks, R. (2010). Development 2.0: the IT-enabled transformation of international development. Communications of the ACM, 53 (4), 22-24.

Holden, S. & Millet, L. (2005). Authentication, Privacy, and the Federal E-Government. The Information Society, 21, 367-377.

Hood, C. (1991). A Public Management For All Seasons. Public Administration, 69(1), 3-19.

Hosein, I. (2004). The Sources of Laws: Policy Dynamics in a Digital and Terrorized World. The Information Society, 20(3), 187-199.

IDRC (2008). Open ICT4D. Archived at: http://www.idrc.ca/uploads/user-S/12271304441Open_ICT4D_Draft.pdf

JRRT (2009). Database State. Joseph Rowntree Reform Trust, London, UK

Kamarck, E. C. (2007). The End of Government . . . As We Know It: Making Public Policy Work. Boulder, CO.

Kettl, D. F. (2005). The global public management revolution (2nd ed.). Washington, D.C.: Brookings Institution Press.

Layne, K., & Lee, J. W. (2001). Developing fully functional E-government: A four stage model. Government Information Quarterly, 18(2), 122-136.

Lessig, L. (2009, October 9). Against Transparency. The perils of openness in government. The New Republic.

Lim, S. S., Cho, H., & Sanchez, M. R. (2009). Online privacy, government surveillance and national ID cards. Communications of the ACM. 52(12), 116-120.

Lyon, D. & Bennett, C. (2008). Playing the ID card: Understanding the significance of identity card systems in D. Lyon & C. Bennett (Eds.), Playing the Identity Card: Surveillance, Security and Identification in Global Perspective. New York: Routledge.

Lyon, D. (2009). Identifying Citizens: ID Cards as Surveillance. Cambridge: Polity.

Morozov, E. (2009, November 30). Turkey tests new means of Internet control Foreign Policy. Archived at: http://neteffect.foreignpolicy.com/posts/2009/11/30/turkey_tests_new_means_of_internet_control

Murakami Wood, D. & R. Firmino. Empowerment or repression? Opening up questions of identification and surveillance in Brazil through a case of ‘identity fraud’. Identity in the Information Society 2(3).

OECD. (2003). The e-Government imperative. Paris: Organisation for Economic Co-operation and Development.

OECD. (2005a). E-government for better government. Paris, France: OECD.

OECD. (2005b). Public sector Modernisation: Open Government. Paris: Organisation for Economic Co-operation and Development.

OECD. (2009). The role of digital identity management in the Internet economy: a primer for policy makers. DSTI/ICCP/REG(2008)10/FINAL. Paris: Organisation for Economic Co-operation and Development.

Sábato, Hilda (2001). The Many and the Few: Political Participation in Republican Buenos Aires. Stanford, Stanford University Press.

Smith, M. & Elder L. (2010). Open ICT Ecosystems Transforming the Developing World, Information Technologies and International Development, 6 (1), Spring 2010, 65–71.

Thill, Eduardo. (2007). Personal interview with Eduardo Thill, Director de Gestion informatica, Ministerio del Interior, Argentina.

UN & APSA. (2002). Benchmarking E-Government: A Global Perspective. New York: United Nations.

UN. (2008). E-Government Survey 2008: From E-Government to Connected Governance. New York: United Nations. Document Number)

United States Executive Office of the President (2009a). Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure, 1-76.

United States Executive Office of the President. (2009b, 21 January). Transparency and Open Government. Memorandum For The Heads Of Executive Departments And Agencies. Washington, DC.

Viner, K. (2009, June). Internet has changed foreign policy for ever, says Gordon Brown. The Guardian. Archived at: http://www.guardian.co.uk/politics/2009/jun/19/gordon-brown-internet-foreign-policy

West, D. M. (2005). Global eGovernment 2005. Providence, RI: Center for Public Policy, Brown University.

West, D. M. (2007). Global eGovernment 2007. Providence, RI: Center for Public Policy, Brown University.

Whitley, E. A. & Hosein, G. (2010). Global Challenges for Identity Polices. Basingstoke: Palgrave.

Appendix 1: Current state of identity card systems in Latin America[4]

Country	**Name of system / card**	**Institutional sponsor**	**Centralized database?**	**Smart cards?**	**Personal info collected and used?**	**Biometrics?**	**What sorts of uses?**	**Forthcoming "upgrades"?**
Argentina	Registro Nacional de las Personas / Documento Nacional de Identidad	Internal Affairs Ministry	Yes	No	Name, date and place of birth, address, marital status, sex, voting "check", signature	Facial image and one fingerprint (right thumb)	Traveling to neighboring countries; proof of identity at private and public institutions; voting	A new DNI system has been proposed, intended to digitize the database, facial image and fingerprints contained in the document.
Bolivia	Registro Unico Nacional / Carnet de Identidad	Ministerio de Relaciones Exteriores y Culto	Yes	No	Name, date and place of birth, address, marital status, sex, signature, profession	Facial image and one fingerprint (right thumb)	Traveling within the country; proof of identity at private and public institutions; voting	A "Padron Electoral Biometrico" will be implemented next December.

[4] Source: Authors' elaboration based on government websites and publicly available information. Note that we were unable to locate data on every Latin American country and have chosen to include our major findings here. Furthermore, some cells are unpopulated because not all information is publicly available online.

Brazil	Registro De Identidade Civil	Justice Ministry - Federal Police	Yes	Yes	Name, place and date of birth, sex, parents' names, signature	10 fingerprints and a facial image (in the card's chip). Facial image, right thumb visible on the card.	Traveling inside the country; proof of identity at private and public institutions; voting	A new eID system was launched in July 2008, to be completed by 2017
Chile	Rol Unico de Identidad / Cedula de Identidad	Servicio de Registro Civil e Identificacion - Ministry of Justice	Yes	No, but the card has a bar code which stores all the information contained in the card	Name, place and date of birth, sex, ID issuance and expiry dates, signature	Facial image and one fingerprint (right thumb)	Traveling inside the country; proof of identity at private and public institutions; voting	-
Colombia	Cedula de Ciudadania	Registraduria Nacional del Estado Civil / Organizacion Electoral	Yes	No, but the card has a bar code containing facial image and fingerprints	Name, signature, date and place of birth, height, blood type, sex	Facial image and one fingerprint (right index)	Traveling inside the country; proof of identity at private and public institutions; voting	New system currently being planned
Costa Rica	Cedula de Identidad (only for people aged 18+)	Registro Civil - Supreme Electoral Court	Yes	No, but has a barcode, which includes the citizen's name and fingerprints	Name, signature, date and place of birth, sex, ID expiry date	Facial image (and fingerprints in the barcode)	Traveling inside the country; proof of identity at private and public institutions; voting	Smart card implementation to commence by 2011

Ecuador	Cedula de Identidad	Dirección General de Registro Civil, Identificación y Cedulación	Yes	Yes	Name, date and place of birth, level of education, sex, signature, marital status, parents' names, date and place of issuance, ID expiry date	Facial image and one fingerprint	Traveling inside the country; proof of identity at private and public institutions; voting	-
El Salvador	Documento Único de Identidad	Registro Nacional de las Personas Naturales / Tribunal Supremo Electoral	Yes	No, but it has a bar code which contains all the information on the card plus parents' names and the card holder's organ donation status	Name, place and date of birth, ID expiry date, signature, address, profession, marital status, spouse's name, blood type, electoral zone code	Facial image	Proof of identity at public and private institutions; voting. It's mandatory for everyone aged 18+ to have a 'DUI'.	-

Guatemala	Cedula de Vecindad	Registro Nacional de las Personas	Yes	No	Name, sex, date and place of birth, ID issuance and expiry date, dates that the ID has been replaced, signature, marital status, type of disability (if any)	Facial image	Proof of identity for all civil and administrative interactions, and those which require an identity check.	Current card is being replaced by the 'Documento personal de identificacion' (only for people older than 18 years old). This process will be finished by January 2011 when the Cedula de Vecindad will be no longer accepted as legal documentation.
Mexico	Multiple cards (Acta de Nacimiento, Carta de Naturalizacion o Documento migratorio)	Registro Nacional de la Poblacion	No	No	-	-	Essential for tax declaration, registering with companies, schools, affiliation to any health system, passport, etc.	The multiple cards are to be unified in the Clave Única del Registro de Población (CURP), which isn't an ID card, but more like a National Insurance Number. There are also proposals for a new national ID card with multiple biometrics, including irises, fingerprints and digitized facial images.
Paraguay	Cedula de Identidad	Departamento de Identificaciones - Policia Nacional del Parguay	Yes	No, but has a barcode with the information on the card	Name, place and date of birth, ID issuance and expiry dates, signature, ID issuance place, sex, address	Facial image and right thumb	Traveling inside the country; proof of identity at private and public institutions; voting	The government has announced the implementation of a new “Sedula de identidad” of MERCOSUR.

Peru	Documento Nacional de Identidad	Registro Nacional de Identification y Estado Civil	Yes	No, but it contains a barcode with biometric information (right index fingerprint)	Name, place and date of birth, sex, marital status, ID issuance and expiry date, signature, voting check, voting zone/area, organ donation status, address	Facial image and one fingerprint (right index)	This is the only acceptable proof of ID for civil, commercial, administrative, legal and judicial acts; voting	New electronic DNI will be implemented in May 2010.
Uruguay	Cédula de identidad	Ministerio del Interior y la Dirección Nacional de Identificación Civil (D.N.I.C.)	Yes	No	Name, place and date of birth, ID issuance and expiry dates, signature	Facial image and one fingerprint (right thumb)	Required for all interactions with public and private organizations	-

Venezuela	Documento de identidad nacional	Servicio Administrativo de identificación, Migración y Extranjería / Ministerio del Poder Popular para Relaciones Interiores y Justicia	Yes	No	Name, date of birth, ID issuance and expiry dates, signature, marital status	Facial image and one fingerprint	-	-