



Identity cards: social sorting by database

David Lyon

Director, The Surveillance Project and Professor of Sociology
Queen's University, Kingston, Ontario, Canada

Overview

Identity (ID) cards connected with large-scale databases are a key item for political debate in the twenty-first century. An increasing number of countries have started to use, or are considering, national ID card systems. The attack on the USA on September 11, 2001 has prompted more to draw up such plans, for example the UK and Canada. Although not all proposals will succeed, this indicates a strong trend towards monopolizing the means of legitimate identification and regulating mobility.

ID cards mark certain persons as members of a nation state and are usually intended to combat fraud and 'terrorism'. While they may contribute to law enforcement in minor ways, such as visa infractions and petty crime, it is far from proven that they can actually prevent determined violence against civilians or fraudulent activity such as identity theft. At the same time, the association of ID cards with databases means that these are systems for social sorting, permitting extensive discrimination between different populations through modes of classification that may include ethnicity and religion. The pressing challenge is to establish systems that avoid exclusionary bias and in which accountability for handling personal data is paramount.

This Issue Brief gives an overview of the main social and technical issues raised by ID cards, particularly in their modern form as electronic systems linked to computer databases. It explains the nature of ID cards and answers key questions about why they are needed, whether they work and who is affected by them, before concluding with an analysis of their likely broad national and global impacts as systems of social sorting.

The special challenge of smart electronic ID card systems

Many people are used to being asked to show, or have 'swiped', various forms of cards to verify identity in workplaces or for travel, shopping, banking or entertainment and leisure. But electronic and 'smart' national ID cards promise much more. They have a programmable chip embedded in them for storing some data that can be linked to a central database. This connection to a central computer database distinguishes smart ID cards from their paper-based precursors.

Such smart cards typically combine several functions in one card, and may be used both to gain access to government services and to connect the holder with a database record. They also tend to include a biometric device, using fingerprints or iris scans along with a photograph. In those places where they exist or are proposed, everyone will eventually be affected. They have deep implications for wider policy, relationships between citizens and the state, and for power relations more broadly.

The debate over national ID cards is not new; they were developed in various countries and at various times—notably during war—in the twentieth century. The British card from the Second World War, for instance, was scrapped in 1952. Today, however, the issue has received further impetus for several related reasons: the logic of trends in processing personal data; rising mobility in a globalizing world; the growing sophistication of new technologies; and changing forms of states and borders, especially in the aftermath of 9/11.

New ID cards are part of a large-scale trend towards ‘social sorting’—classifying and profiling groups of people in order to provide different services, conditions or treatment. Specifically, new ID cards are intended to include those designated as ‘eligible members’ of nation-states and to exclude undesirable others.

It is misleading to speak only of ‘cards’, as they are actually ID card *systems* in which the card is the portable token of eligibility or membership and the population database to which it refers permits sorting and classification. This combination of ID cards issued to citizens and short- or long-term residents together with the personal information stored in the national database constitutes new ID card systems, in which the networked databases to which the cards link present other issues of power, responsibility and accountability.

ID card systems are part of an emerging new direction for governance that affects many countries. Questions of justice and fairness may be obscured, say within immigration departments, as these practices are automated and integrated. Discretion usually benefits those claiming refugee status, for instance. Automation reduces personal contact.

The necessity of carrying a card presents some important concerns affecting the daily experiences of card holders. Identity and identification are basic social issues in which everyone has a stake, and everyone wishes to have a say. This is the case in the virtual spaces of the Internet as well as in mundane everyday life. Indeed, the use of electronic technologies means that all manner of ID checks are increasingly delocalized. While passports are generally used for crossing geographical borders of nation-states, ID cards mean that the border is everywhere. In other words, the physical border is no longer the only challenge, as the experience of being counted as an insider or an outsider can be reproduced anywhere. The portable card with its virtual referent in the population database produces ubiquitous ‘borders’ (Lyon 2004).

As soon as identities are checked in order to categorize and profile people, resistance tends to grow. Our subjective sense of identity is challenged when outside identification procedures classify us in ways we dislike or dispute. Beyond this, ID card systems have the potential to entrench negative discriminatory practices and to enhance the power of those who can manipulate the technology. As Elia Zureik (2004: 130) points out, ‘By using biology and physical appearance as a means of identification, biometrics are likely to legitimate group differentiation and racialization in society in the name of security’. At the extreme end of the spectrum, ethnic classification on ID cards was directly connected with twentieth-century genocide in several countries, including Rwanda (Fussell 2001).

From a policy point of view, much more care should be taken with personal data because people's life-chances and choices are affected in such crucial ways. However, part of the problem is that populations for whom cards are being provided often do not know exactly what is going on and thus the processes of establishing card systems are deficient, democratically speaking.

What are ID cards?

ID cards are, by definition, markers of membership; national IDs show that their holders are legally in a country, with a right to work, receive health care, education and other benefits. For example, 'Entitlement Cards' in the UK or 'Permanent Residents Cards' in Canada show that their bearers are eligible for certain advantages—such as health care—only granted to citizens and particular other residents. If the new British ID card scheme is successfully implemented, Entitlement Cards will be phased out.

While many countries have ID cards that simply verify identities in relation to a numbered registry, the ones discussed here are mainly of the new smart-card type. Without adequate safeguards, the way these new cards lend themselves to multiple-purpose usage could result in greater overall surveillance capacity, particularly within the nation-state.

The other side of the coin is that cards also regulate identity and mobility. The search for stable means of identification has been under way since early modern times, with the movement starting in France, where 'scientific' means were sought for this (Piazza 2004). The idea was to try to fix the category of 'legitimate identity' and to distinguish it from other claims originating in families or religion. In the late nineteenth and early twentieth centuries, this meant experiments with 'anthropometrics', such as head measurements, to distinguish different classes of citizens. But ID cards also reinforce a pervasive trend, especially in the twentieth century, in which states increasingly assert their monopoly over the means of movement. The passport is the conventional way of doing this. Yet, even in a globalizing world, obtaining a passport is a voluntary act taken only by those who wish to travel outside the borders of their country. The idea of a compulsory ID card ensures, in principle, that all citizens have cards to provide a means of demonstrating that they are who they claim to be.

ID systems currently being discussed and set up depend on having a database of personal information that must accompany the cards. In the UK, the plan is to establish a National Identity Registry, the database of personal information to which the biometric cards would link (Home Office 2003). The cards will use facial recognition, iris scans or fingerprints and these data will be stored in the system along with name, date of birth, address and other basic personal information. This continues a long-term trend of computerizing government departments, which has been going on since the 1970s but is now significantly amplified by network-searchable databases that automate the process of checking whether eligibility criteria for benefits and services have been met in each case (Lyon 2001).

Why are ID cards needed?

We live in an era where travel and tourism occur routinely on a very large scale, for instance with about 90 million visits each year made to Britain via seaports and airports and travel occurring on a similar scale elsewhere. In this context, automating the checking process to decide which visitors may work, claim medical benefits or remain in the country after a set period of time is a very attractive idea. At face value, ID cards therefore seem to make sense. Nevertheless, whether or not ID cards are really needed depends, of course, on what is expected of them. And expectations vary from country to country, and even within countries.

At least three kinds of arguments are used to promote ID systems; eliminating terrorism, preventing fraud and controlling immigration. The first works on the logic of security and fear, the second on that of management and audits and the third on legal residence—who may be in the country and what they may do while there. ID cards, it seems, can provide simultaneous solutions to several perceived problems. The key is to distinguish reliably between one category of persons and another in order to treat each appropriately.

Ostensibly, new ID card systems are rolled out—to use the misleadingly simple-sounding jargon—to meet these expectations. Firstly, ID systems are supposed to distinguish between peace-loving and potentially violent members of the community and thus to pre-empt repeats of the events of 9/11. Secondly, ID cards are intended to prevent ‘identity theft’, credit card fraud and false claims to medical or health benefits. They tighten controls, making it harder for ineligible persons to claim services or benefits. A third set of justifications has to do with immigration controls. In a world where territorial borders have become more and more porous, such as in the European Union, means are sought to regulate as well as to facilitate the flows of foreign nationals. Being ‘British’ or ‘Japanese’ or ‘Indian’ is increasingly formed from surveillance practices in general, censuses and population registers in particular.

The first justification, eliminating terrorism, appears to have contributed much to the political acceptability of ID cards among populations (such as the British) where there was resistance hitherto. Ironically, this is the area in which the answer to the question ‘Will the cards work?’ is most moot. On the other hand, one could argue that the second level of justification relating to identity is both understandable and, in many cases, socially and politically acceptable. However, whether a very expensive national ID card is needed to deal with the problem is another question. The assumption seems to be that a single means of correctly assigning identity is handy, convenient. The justification of controlling immigration is probably the oldest rationale for national ID systems and the one that is most shared among the various countries that already have, are implementing or are debating ID systems. That it is also the most controversial is sometimes obscured by the currently loud rhetoric of ‘security’ and the apparent ‘common sense’ of upgrading administrative systems and managing risk.

Old fashioned ID cards, such as those in France, have ‘worked’ for some purposes over many decades. As Gerard Noiriel (1996: xix, 45–90) points out, from the beginning, in the 1890s, the ‘card and the code’ went together. The national identification card was intended to keep certain categories of people from settling illegitimately in France and the Nationality Code provided the categories that distinguished them. Crucially,

a distinction was made between 'immigrant' (undesirable) and 'tourist' (desirable, or at least tolerated), along with other classifications. But the cards have not 'worked' in a simple sense. A hundred years after they were introduced, one third of the people living in France have foreign-born parents or grandparents. True, such immigrants have been obliged to assimilate in order to survive and, equally true, the far Right has been increasingly vocal and active against immigration and immigrants in France since the 1980s. But the cards and the code have played a role in maintaining some of the distinctions laid down in the nineteenth century.

Writing about the history of the passport, John Torpey (2000) suggests that it is the symbol of the 'monopoly of the means of movement' sought even more stringently by nation-states in an era of high mobility and globalization. In parallel with this, I suggest that national ID cards speak more of the desired state monopoly of the 'legitimate means of identification' because they help to sort the 'national' from the non-national other. As the card and the code go together, producing a card presumes the existence of a code that provides the categories by which people are placed in one group or another. And the code, of course, is fluid, changeable and contestable. Fear of certain kinds of crime, immigration policies and panics about 'terrorism' all have an effect on the codes.

Do ID cards work?

The pragmatic version of the ID card question—"Do the cards work?"—has to do with their technical reliability rather than their effectiveness in maintaining national identity, such as the 'Frenchness' of France. A common thread from the earliest ID cards in Europe to the present has been to try to ensure the efficiency and security of identification papers. The quality of the paper and ink, the use of watermarks and other devices were intended to guarantee the integrity of the system. As noted earlier, there was also an emphasis on physical identifiers, from anthropometrics and photography to fingerprints. The reason given for the 'workability' of the ID card systems being introduced today is that biometrics are used in conjunction with the national registry database and that the cards themselves have various 'tamperproof' features. Among these, biometrics appears as the holy grail.

It is a mistake simply to think of biometrics as something 'new', a product of 'recent' technologies. Prints in hardened clay identified potters in ancient Egypt and property deeds in ancient China were authenticated by fingerprints. In nineteenth-century India, palm prints were used for contracts and Alphonse Bertillon introduced his anthropometric techniques in France to identify habitual criminals (Didier 2004: 36). In the early twentieth century, telegraph operators developed codes enabling them to be recognized, and in the 1960s the American Federal Bureau of Investigation (FBI) attempted to automate fingerprint processing. At the same time, Stanford University used hand measurements to check entry to examination halls.

To secure a system, biometrics specialists insist, both identification and authentication should occur. Identification describes uniquely each person in a known population to demonstrate whether or not that person is a member of the population. In other words, one individual's description is compared to all other individuals' descriptions. Authentication, on the other hand, requires a trusted third party to verify whether or not

the person fits the authentic description. This can be achieved using a memory in a file, or a medium such as a smart card. In this case, the identity is not implicated; it is a one-to-one comparison of descriptions. Biometrics will always offer authentication, but not necessarily identification. This is why person-specific data—such as fingerprints, and now face-scans, iris scans or DNA—are required.

While this sounds like steady technological ‘progress’, problems are still presented. DNA may be reliable but it would be impossible to use body fluids for routine airport checks, for instance. Iris scans are believed to be the most reliable of the current options, but even these have drawbacks. For example, Nordic people have pale irises, some Africans have very dark ones—so not all populations can be registered in the database. This is known as ‘failure to enrol’. Beyond this are ‘false match rates’—say, a ‘watch list’ in which a false identification is made with an individual who is to be excluded. The higher the setting of the system towards blocking all impostors, the more people will be mistakenly blocked. This means that, for example, airports simply cannot afford to have high settings to check passengers because the number of alarms would quickly make the airport grind to a halt.

All these issues, to do with enrolment, false match rates and false non-match rates, are highly specific to the technical aspects of the biometric system for ID cards. Broader issues, as raised for example by the Electronic Privacy Information Center (EPIC) in Washington DC, also affect the successful working of biometric systems. EPIC (2003) stresses that the degree of centralization or decentralization of systems is important; in principle, smart ID cards may be used in a decentralized system that reduces the amount of personal data in a central file. The security of the system itself is significant, as is the degree of confidence in the process of authentication. A large question hangs over where decisions are taken about linking biometric data to other records, such as those held by police or marketing companies. Lastly, the EPIC document raises the question of ‘unintended social consequences’ of introducing unfamiliar systems. In the case of biometric ID cards, it is simply not known what the long-term effects will be of further inserting the citizen into the machinery of electronic administration.

Who has ID cards and why?

Citizens of several countries around the world already carry smart ID cards. Existing schemes fit, in various ways, with degrees of democracy, economic liberalization and the desire to demonstrate technological prowess. And while ID card proposals may be ‘new’ in the UK, there are unsuccessful commercial precedents, such as the ‘Mondex Card’ which was promoted as a kind of ‘electronic cash’ when tested in the mid-1990s in Guelph, Ontario and Swindon, UK. Interestingly, the most significant developments are in South East Asia, where China, Hong Kong, Thailand, Malaysia and Singapore either have smart ID cards or are soon to establish them.¹ With the exception of Hong Kong, the cards were developed or implemented with little consultation or public objection (curiously, the Hong Kong card is based on ‘Multos’, the Mondex technology). These are far from fully democratic countries. The onus is on those who propose new ID card systems to demonstrate that they will not exhibit authoritarian tendencies in practice.

The largest program ever is being launched in China: an electronic card to replace the current credit-card size laminated document. Eventually, vital information on all 960 million eligible citizens will be stored on chips that authorities anywhere in the country can access. As in other countries, it is hoped that the cards might help eliminate fraud, but in China an additional justification is to try to halt the rural–urban drift. The exact specification of the cards is as yet unclear. High-tech protections are promised but how these will work is equally obscure. Skeptics argue that the new card may well provide another means of social and political control.

In some countries, governments have tried and failed to introduce multiple-purpose cards. In each case, the popular outcry against these schemes helped to prevent their implementation. The ‘Australia Card’ was proposed back in the mid-1980s, and was defeated as unnecessary and potentially authoritarian in 1986. A similar debacle occurred in South Korea in the mid-1990s, when the ID card became an election issue and its opponents were voted into power. More recently, a coalition successfully fought against a smart national ID card in Taiwan. More quietly, a Canadian national ID card proposal was scrapped during 2004.

The situation is different in Japan, however, where a computerized national ID has been launched. It compiles the personal data of citizens into a central database accessible by government. Vocal opposition to this project is ongoing. In Europe, Austria, Belgium, Germany, Russia and Spain are keen to establish similar systems. Spain in particular sees it both as a security device—in a country where Basque terrorism was known long before 9/11—and as proof of superior high-tech capacities.

Opinion polls have suggested Americans are unenthusiastic about national ID cards, even though the driver’s licence or Social Security Number often function as surrogates (Dutton and Meadow 1987). In 1993, for instance, only 39% of Americans were in favour of ID cards while 53% objected to them. But in the immediate panic regime generated by 9/11, 70% of Americans seemed ready to countenance ID cards, one of several straws clutched as an antidote to fear, and only 26% objected. Ironically, the chances are that the ID cards may appear through the same system that already provides some *de facto* elements—the driver’s licence. A current plan is to unify the state-run system into a grand electronic network, and to enhance the capacity of cards for commercial as well as government purposes.

There does seem to be a global trend towards deploying a full-scale smart national ID card based on biometrics that offers multiple uses, but for varying reasons and with different outcomes. The common factor, however, is the desire to regulate or restrict the activities of designated undesirable or ineligible persons. Alongside this, the temptation to technical showmanship is strong, and corporations are understandably enthusiastic to obtain lucrative contracts. Media-amplified fears of ‘terrorist’ attacks are also a powerful motivator, especially in the USA. But the association of several such schemes with authoritarian tendencies, and with disregard for civil liberties, is hard to ignore. Under other circumstances, those who first introduced new cards would not be seen by Western countries as democracies to emulate.

What is the broader context of ID cards?

It is clear from the brief survey above that countries with new smart ID cards are likely to have reasons for wanting to discriminate between legitimate and illegitimate groups: claimants to state benefits, asylum seekers, migrant workers, tourists and students. The current UK ID card proposal suggests that, while the factors of so-called cybercrime and identity theft on the one hand and anti-terror on the other are important rationales, regulating immigration still appears to be central.² This fits with the broader European context, in which checking asylum seekers and illegal immigrants is key to the quest for biometric IDs and passports. In the USA, while worries about illegal immigration and drug smuggling are high on the list of reasons for adopting common biometric standards in passports, the 'anti-terror' agenda is still the most telling.

Whatever the case, it is unclear how negative discrimination against already marginalized and disadvantaged groups will be avoided by the use of national ID cards. The history and current use of ID cards outlined here suggests this, as do the justifications for their introduction in the climate of fear and suspicion following 9/11. Immigrants and refugees often have little or no voice with which to speak out against border-crossing experiences, which can be profoundly negative. Even Canada, with its positive human rights record, is still dealing with the case of the Ottawa engineer Mahar Arar, a Canadian citizen, tortured in detention after being deported from the USA to Syria in 2002. Since 9/11, a number of Arab and Muslim groups have made official complaints about their treatment at borders, by police or in city neighbourhoods. And in an Ipsos-Reid poll in 2004, 41% of Canadians felt they would not be fairly treated by security forces if they were wrongfully accused of terrorist activity (CTV.ca News Staff 2004).

With the use of biometric ID cards, the codes that determine the status of those who hold (or do not hold) the cards are increasingly related to bodily and behavioural characteristics. This further abstracts from the narratives of ordinary life and struggle experienced by those who are most vulnerable. As Didier Bigo (2004) suggests, biometric ID cards produce not so much a *panopticon* as a *banopticon*. In other words, they are not meant to put all under scrutiny, but to single out the exceptions as quickly as possible. Profiling to discover differences, the banopticon channels flows of information in order to control at a distance any who deviate from the coded norms. Skin colour, accent, attitude—these may all be used to assign worth or risk, such that 'hazards' may be removed swiftly. The multiplication of stories of those who have been wrongfully apprehended, detained and even tortured since 9/11 only serves to underscore the dangers of automating such processes.

The state has taken great interest in these questions—of law and order, insiders and outsiders—because it is one area where it still has a voice, after losing several of its erstwhile functions in the deregulation spree of the 1980s and since. So, states are likely to see ID card systems as intrinsically attractive. They can keep out unwanted foreigners in an economical way and also help to stimulate technology-dependent economies. Far from being a means of ensuring greater social cohesion, however, the evidence presented here suggests that ID cards will aid the processes of profiling and classifying, thus accentuating difference. Moreover, unless there are some very stringent safeguards in place, the combination of ethnic and racial criteria that go into

the classification process, along with the use of physical markers on which biometrics depend, augurs badly for multiculturalism and cosmopolitanism.

At the same time, if they recognize the ID card systems for what they are, citizens are unlikely to accept new ones without a struggle. The processes of identity formation and of identification touch some of the deepest areas of human life. Who we are and how we relate to others are basic social questions on which much, including life or death, may hang. More mundanely, people may simply not wish to have their daily activities and movements so constantly monitored and tracked by networked computers for government departments. The perceived risks to ordinary people, from what the new ID systems would seem to permit and authorize, are just too great.

In the long term, the struggle will probably be over the details and the safeguards, rather than whether or not any ID system is installed. That being so, the debate must focus on the accountability of those processing the data, and on hugely enhanced protection for those whose data are handled by others.³ This will be a central struggle in the information politics of the twenty-first century.

References

- Bigo, D. (2004) Globalized In-security: The Field of the Professionals of Unease Management and the Ban-opticon. *Traces: A Multilingual Journal of Cultural Theory*, 4.
- CTV.ca News Staff (2004) Uneasy About Security–Rights Balance: Poll. Scarborough, Ontario, Canada: CTV.ca. www.ctv.ca/servlet/ArticleNews/story/CTVNews/1076289101731_6/?hub=CTVNewsAt11
- Didier, B. (2004) Biometrics. *The Security Economy* (OECD: Paris).
- Dutton, W. H. and Meadow, R. G. (1987) A Tolerance for Surveillance: American Public Opinion Concerning Privacy and Civil Liberties. In Levitan, K. B. (ed.), *Government Infostructures* (Westport, CT: Greenwood Press) pp. 147–170.
- Electronic Privacy Information Center (EPIC) (2003) *Biometric Identifiers* (EPIC: Washington, DC). www.epic.org/privacy/biometrics/
- Fussell, J. (2001) 'Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing'. Presentation to the Seminar Series of the Yale University Genocide Studies Program, 15 November. www.preventgenocide.org
- Home Office (2003) *Identity Cards: The Next Steps*, Cm 6020 (London: Home Office), November. www.official-documents.co.uk
- Lyon, D. (2001) *Surveillance Society* (Open University Press: Maidenhead, UK).
- Lyon, D. (2004) The Border is Everywhere: ID Cards, Surveillance and the Other. In Zureik, E. and Salter, M. (eds), *Who and What Goes Where: Global Policing and Surveillance* (Willan: Cullompton, UK).

- Lyon, D. (2005) *La Frontière est Partout: Encartement, Surveillance et Altérité. Les Cahiers de la Sécurité Intérieure* (forthcoming).
- Noiriel, G. (1996) *The French Melting Pot: Immigration, Citizenship, and National Identity* (University of Minnesota Press: Minneapolis).
- Piazza, P. (2004) *Histoire de la Carte Nationale D'identite* (Odile Jacob: Paris).
- Torpey, J. (2000) *The Invention of the Passport: Surveillance, Citizenship and the State* (Cambridge University Press: Cambridge).
- Zureik, E. (2004) (with Hindle, K.) Governance, Security and Technology: The Case of Biometrics. *Studies in Political Economy* 73:113–137.

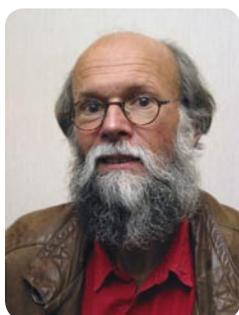
Notes

¹ Some details about ID cards in different countries can be obtained from Privacy International (www.privacy.org/pi/activities/idcard/idcard_faq.html).

² In Home Office (2003: 4), 'illegal migration and working' are mentioned before 'organized crime and terrorism, identity theft and fraud and fraudulent access to public services'. However, the latter phrase is qualified by '...for example by illegal migrants who have no entitlement to them'.

³ This raises important educational and policy questions, such as those to do with privacy-enhancing technologies for the Internet, data protection and freedom of information. These are too numerous to explore within the space available in this Issue Brief.

About the Author



David Lyon is Director of The Surveillance Project and Professor of Sociology at Queen's University, Kingston, Ontario. The transdisciplinary and international Surveillance Project examines the social, political, economic, cultural and legal aspects of processing personal data, and relates these to policy debates (www.queensu.ca/sociology/Surveillance). He is author and editor of a number of books, including *Surveillance after September 11* (Polity Press 2003) and *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (ed., Routledge 2003); he is currently working on an introduction to surveillance studies and the third book in a surveillance trilogy that follows *The Electronic Eye* (Polity Press 1994) and *Surveillance Society* (Open University Press 2001).

The key to ID cards: 'identity card usages', not 'identity usages'

Comment 1 on *Identity cards: social sorting by database*
(David Lyon, OII Internet Issue Brief No. 3, November 2004)

Etienne Combet
President, e-Forum

In his OII Issue Brief on identity (ID) cards, David Lyon outlines the main issues at stake and explains the nature of identity card systems. Here, I would like to add a few observations, particularly in terms of the significance of aspects of ID card usage, such as cost–benefit analyses.

The main reasons for the current interest in ID cards

Three reasons make identity cards a topic of great interest now: more countries are starting to use them; there is strong pressure to include biometric data for anti-terrorism and police purposes; and the time has now come when the capabilities of electronic chips relating to electronic identity are ready to be used, for example for electronic authentication and signature.

On the first issue, I would just comment that this question has already been solved—although many citizens and governments may not know it. What country does not have a material way of knowing who is entitled to stay on its territory? This can be a driver's licence, a resident's card, a birth certificate, a proof of tax payment, of health insurance, of a right to work...or a combination of two or more of these. Obtaining and carrying such proofs are more or less difficult or expensive. An identity card is usually a 'secured' card, given to an identified citizen after a face-to-face interview, during which he or she produces appropriated proofs. Its main usage is similar to the use of passports: allowing citizens free, but potentially controlled, circulation in authorized areas.

On the second issue, adding biometric data is a way of controlling more securely the matching of information in the card with the bearer, both for the bearer's benefit and the benefit of his or her counterpart. Questions relating to the constitution of a database of this personal, and eventually biometric, information are of an ethical nature, with the fine tuning between security and liberty to be decided by concerned populations. Usually, a minimum of centralization is required for efficiency, which raises appeals for new laws to protect privacy.

Secondary usages tend to be found when a 'transportable identity form' exists somewhere; for instance, showing a driver's licence is a condition to write a cheque in the USA. In France, the real development of (non-mandatory) identity cards started with the development of paper cheques. By securing a higher level of certainty about the identity of bearers, electronic means of identification could allow higher confidence in the usages enabled by ID cards. In turn, this would help e-business and

e-government, in a similar way to the assistance given by post-war paper identity in developing post-war economies and government. This third issue may appear simpler, but raises many unsolved questions.

Understanding economic factors

Electronic identity cards are coming, but economic factors still have to be clearly defined. Individuals usually resist the idea of a single ID card that includes all information about themselves under their 'unique number'. On the other hand, their wallets offer a too-limited space to carry one card per usage. As a result, many experts forecast that individuals will carry one card for health and insurance usages, one for banking and payments, one for professional usages, one for personal government identification, and eventually one or two more.

Three simple questions to this key issue should be raised:

1. What important usage can be offered through an electronic identity card that is not available without a card?
2. What are the costs of:
 - a) implementing such a system;
 - b) distributing cards to millions of bearers;
 - c) granting bearers secured online access (e.g. through computers, Internet links, and card readers); and
 - d) developing and maintaining applications defined in Question 1?
3. Are the savings identified in Question 1 higher than the costs of Question 2?

If the answer to Question 3 is 'Yes', you have just found a model that can support the implementation of electronic identity cards.

The development of this kind of practical insight to significant questions about e-government, such as those surrounding electronic identity cards, is an important part of the mission of e-Forum, a non-profit organization involving academic researchers, industry professionals, and local and central government managers across Europe (www.eu-forum.org). Launched and financed by the European Commission in 2001, its purpose is to identify best practices in e-government and to disseminate them through conferences, practical working groups, research papers, targeted learning journeys, and participation in European research projects.

Time to ask questions about the paths opened by ID cards

Comment 2 on *Identity cards: social sorting by database*
(David Lyon, OII Internet Issue Brief No. 3, November 2004)

James B. Rule

Professor of Sociology, State University of New York, Stony Brook

It's easy to see why governments around the world are so intent of late to impose ID card systems on their populations. People in many countries have come to perceive themselves in danger from sinister human forces—terrorists, illegal immigrants, unworthy claimants for public benefits. Governments have managed to frame these dangers as curable, if only state agencies can get a more effective grip on who is who.

This is certainly hype, but not necessarily all hype. No one doubts that there are dangerous actors about, or that many people claim statuses or privileges to which they are not officially entitled. The question is, will the real consequences warrant the massive, far-reaching shift in relations between governments and governed that will be triggered by these systems?

In response, all of us—social scientists, computing specialists and others whose work focuses on the interaction between human systems and information systems—should do just what David Lyon does in his OII Issue Brief on identity (ID) cards. We should ask, first, whether the proposed systems will really have the felicitous effects touted for them. In addition, we should ask what *other* effects the imposition of such systems will have, particularly non-intuitive second-, third- and *n*th-order consequences that are unlikely to be broached in public debate.

Intended effects of ID cards

Regarding intended effects, the claims are well known. But are they credible? Will they prevent further terrorist acts? How? Does the danger of such attacks lie in the fact that the perpetrators are not really who they say they are? Or are such actions more likely to be the work of people who are who they say they are, and whose 'papers are in order', but who harbor intentions that the authorities have not yet attributed to them? Similarly, with regard to illegal immigration: how many persons illegally residing in any country are likely to be identified by use of identity cards, who could not be identified by other means? And are state authorities really prepared to apprehend all these 'undocumented' aliens betrayed by their lack of proper identity cards and deport them? In my own country, the United States, I believe the unavowed answer to this latter question is negative. When one tries systematically to anticipate the actual benefits of putting ID card systems into use, the projected gains appear less and less certain.

Unintended or unacknowledged consequences

There are also the unintended—or perhaps simply officially unacknowledged—consequences that are apt to flow from ID card imposition. As David Lyon's Brief reminds us, national adoption of ID cards doesn't just amount simply to the dissemination of discrete *things*. It also involves the creation of sweeping new systems of communication and enforcement. It's not just the information appearing on the card that will be disseminated, nor indeed just what is contained on any chip embodied in the card. Instead, creation of the system will mean exposure of ID card holders to scrutiny from any institution successfully claiming legitimate access to encompassing, computerized systems of checking, matching and acting. What institutions, what interests, will be able to participate in these processes?

We take it for granted that persons urgently wanted for arrest will be instantly identified when their ID cards are scanned or otherwise checked against the system. But what other interests and institutions will have the right to enforce their claims in this way? Will civil courts be empowered to use such systems to track spouses who abscond on child-support orders, and in so doing to enforce such orders? Will it be possible to check the identities of ID-card holders against lists of those suspected of bearing highly communicable diseases—or those convicted of child molestation, spousal abuse or others judged to pose special dangers to 'society'? Once such a system exists, it will be extremely difficult to resist demands that any 'legitimate' social obligation be enforceable in this way.

The start of an unpredictable journey

The point is, ID card systems, like other new technologies, will not just be socially neutral 'tools' for achieving aims that everyone seeks. They will set in motion whole new sets of social relationships—new opportunities to enforce obligations and claims in realms where anonymity once prevailed. No one can claim to know with certainty what the full list of such claims and obligations will be, or who will make up the legitimately authorized 'enforcers'. What we can be sure of is that creation of such systems will mark the beginning of a long, contentious journey from which it will be difficult, if not impossible, to turn back.

Now is the time for people like us to be raising these issues.