IDENTITY CARDS
A GLOBAL PERSPECTIVE

High-tech ID systems, incorporating smart cards, biometrics and radio-frequencies and connected to mega-databases to track our every movement, are being introduced simultaneously worldwide. Is this a coincidence?

by Nathan Allonby
© Global Research
31 August 2009

Centre for Research on Globalization
Montreal, Canada
Website: www.globalresearch.ca

Electronic identity (ID) cards have made alarming progress towards becoming universal around the world. Already, over 2.2 billion people, or 33 per cent of the world's population, have been issued with "smart" ID cards. Of those cards, over 900 million have biometric facial and fingerprint systems. On present plans, over 85 per cent of the world's population will have smart ID cards by 2012. Most of the remaining population won't have escaped: largely, they are already enrolled in earlier-generation ID systems, often in repressive states such as Myanmar (Burma).

Understandably, campaigns against the introduction of ID cards have tended to play up the problems with ID systems, presenting them as being unworkable and creating unmanageable problems with privacy invasion, fraud, unauthorised database access, organised crime, unreliability of biometric recognition, etc. As a result, a substantial number of people believe mandatory ID cards "just won't happen".

It's long past time to stop burying our heads in the sand. There are no obstacles to the worldwide introduction of mandatory electronic ID cards.

All those problems with ID systems may be real, but they are not enough to stop implementation, primarily because these are problems that will affect people as individuals, not their governments—our problem, not theirs. There has been hardly any meaningful debate about one of the biggest issues of our time.

It's also time to look at what ID systems are really intended to do, not at the public justification for them. Since governments probably always knew that ID cards wouldn't stop terrorism, organised crime, ID theft, fraud, etc., there has to be some other reason for their introduction—and it appears to be a reason that governments don't want to own up to in public.

A Coordinated International ID Agenda?

Perhaps we can learn more if we look at what is going on around the world. Interestingly, nobody seems to have published a comprehensive or reliable survey of worldwide ID schemes, so a survey had to be compiled for this article [see tables in author's original posting; Ed.].

What stands out from this survey, incomplete as it may be, is that advanced electronic ID card systems are coming to some of the poorest nations in the world, some in chaos, civil war and starvation, both small and large countries. They are coming to nations with vastly divergent cultures, to nations that are almost completely pre-industrialised and underdeveloped, and coming first to almost all Islamic nations. The few that will not have advanced electronic population registration will be in a tiny minority. This is all to happen by the end of 2012. For example, on 25 June 2009, India announced it is pressing ahead with the introduction of universal biometric ID cards, to be completed by 2011—to register nearly 1.2 billion people within just 18 months.

However, there are grey areas. For example, in some states, such as Mozambique and Zambia, there are biometric ID cards for voter registration which aren't officially national ID cards but nonetheless have registered the population.

"Election cards" tend to become national ID cards immediately after an election, as in Haiti. (How did introducing ID cards get linked to "bringing in democracy"?) The USA would probably be in the grey area due to the uncertainty (deliberately not clarified) about the Real ID Act, Canada due to proposals for biometric "enhanced drivers licenses", and Australia due to the uncertain status of the Access Card. Any uncertainty gets put into perspective by the "big picture": ID cards are coming, almost everywhere.

The simultaneous introduction of very similar ID card systems in so many nations seems more than a coincidence. If it were purely a matter of nations taking their own initiative to upgrade systems, this would happen over a longer timetable as nations periodically updated systems once every couple of decades. Does this timetable indicate unseen international pressure applied to nations to adopt ID cards?

In the process of researching the list, something interesting came out. The plans to introduce a national ID card system in Uganda were announced in a memorandum of understanding, dated 20 June 2008, sent to the International Monetary Fund (IMF).

Has the IMF required nations to adopt biometric ID cards, on the pretext of instigating financial regulation and preventing fraud and money laundering?

The impression is that the IMF was involved in the decision long before the people of Uganda were consulted about their national ID card scheme.

Has the IMF required nations to adopt biometric ID cards, on the pretext of instigating financial regulation and preventing fraud and money laundering?

Again and again, in the public description of the alleged benefits of biometric ID systems, the reasons given include the benefit to the banking system, in preventing fraud, and allowing the poor to have access to the banking system.

Several nations (e.g., India) have mentioned the need to confirm that aid gets to the intended recipients and is not lost in fraud—again, something which a body such as the IMF might see as a justifiable reason to promote or require biometric ID, but other people would see as a mere pretext for "policy laundering".

In a different example of western promotion, the European Union (EU) has financially sponsored the introduction of biometric ID cards in the Democratic Republic of Congo, allegedly to help promote peace by tracking down ex-soldiers and ex-fighters. A similar logic has been applied to a biometric scheme in Somalia.

Grotesquely, biometric ID cards are coming to Rwanda. ID cards were a major tool in the Rwandan genocide. Imagine how much more effective the genocide could have been with a computerised population register and an ID system with biometrics to prevent fraud or evasion. Rwanda's experience is an horrific illustration of how lethal ID cards can be in a nation in civil war, and raises uncomfortable questions about western involvement, as does the situation in Congo.

Policy Harmonisation in the EU, UK and USA

The worldwide introduction of ID cards is merely the visible witness of an invisible process. Policies that profoundly affect our lives and take away our freedoms are worked out in secret international deals.

In July 2005, during its six-month rotation in the Presidency of the EU, the United Kingdom introduced a proposal for biometric ID cards for Europe despite the fact that it had no power to do so under the EU treaties at that time.

Legalities being no obstacle, this subsequently evolved into binding EU policy in the Hague Programme on justice and security.

However, policies introducing ID cards, evolved in secret, go far beyond identification and security, as described by Tony Bunyan of Statewatch in an article in the *Guardian* ("The surveillance society is an EU-wide issue", 28 May 2009; includes quotations from Bunyan's Statewatch report, "The Shape of Things to Come"). ID cards are only one tool, enabling a much larger scheme to track and record the life of every individual; Bunyan calls this the "digital tsunami".

> *'Every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations', leading to behaviour being predicted and assessed by 'machines' (their term) which will issue orders to officers on the spot. The proposal presages the mass gathering of personal data on travel, bank details, mobile phone locations, health records, internet usage, criminal records however minor, fingerprints and digital pictures that can be data-mined and applied to different scenario[s]—boarding a plane, behaviour on the Tube or taking part in a protest.*

But this isn't just coming to Europe, as Bunyan explains, because the USA and Europe will share similar policies and practices in an agenda of policy harmonisation:

> *...it is proposed that by 2014 the EU needs to create a 'Euro-Atlantic area of cooperation with the USA in the field of freedom, security and justice'. This would go far beyond current co-operation and mean that policies affecting the liberties and rights of everyone in Europe would not be determined in London or Brussels but in secret EU–US meetings.*

Was this a response to 9/11? No, emphatically not. We can say this because some of these schemes have a published history and timeline dating from much earlier, e.g., Taiwan, 1997, and India, 1999. We can trace a continuing pursuit of ID-based databases back to the Australia Card, which was defeated in 1987. We can also say with certainty that EU–US cooperation on security pre-dates 9/11, as does EU development of security databases which have been applied to political protestors.

What Do ID Cards Do?

The new cards are like a high-tech "glue", an interface, joining together all the different state databases and linking their information together. This is the significance of the "multi-functional" identity function of the new cards: one ID number is the key to access all services and also all databases. One card, one number, tracks a person across multiple activities, across their whole life and everything they do—employment, tax, health, everything. When numerous databases are linked together by means of a common interface, in this case ID numbers, they effectively function as a single "meta-database".

...one ID number is the key to access all services and also all databases... When numerous databases are linked together by means of a common interface, in this case ID numbers, they effectively function as a single "meta-database".

In the *Guardian* (30 September 2003), home affairs editor Alan Travis wrote that the "citizen information register" in Britain will "bring together all the existing information held by the government" on its 58 million residents:

> *It will include their name, address, date of birth, sex, and a unique personal number to form a 'more accurate and transparent' database than existing national insurance, tax, medical, passport, voter and driving licence records...*
>
> *The decision to give the go-ahead to the national population register without any apparent need for new legislation or any public debate is in sharp contrast to the intense cabinet debate now taking place over the...identity card scheme...*
>
> *...The scheme is a joint project between the Office of National Statistics and the Treasury...*
>
> *The idea was developed by the Treasury's public services productivity panel—a group of senior business people and public services managers...*
>
> *[The Home Office] admitted a national identity card scheme will have to be 'underpinned by a database of all UK residents' and asked for views on whether the citizens information register should be used for this purpose...*

The Indian ID scheme is another major example. According to an article in the *Hindu* (26 June 2009):

> *...the UID [Unique IDentification] numbers and the database will be linked to agencies such as the Election Commission of India and the Income Tax Department, which...issue...voters photo identity cards...*
>
> *In addition, it will be used for providing services under government schemes such as the public distribution system, and the National Rural Employment Guarantee Scheme for families living below the poverty line...and for delivering financial and other assistance to the needy.*

This is the new model for e-government around the world. Historically, this isn't the first time we have seen systems like this. It is very similar in concept to the Nazi ID system, as it finally evolved, with a Reich Personnel Number to link all other databases.

The system of compiling the initial population register from records in existing, earlier databases is, again, very similar to Nazi practice.

Why should this be significant? Why should there be any big deal about the government collecting together data that it already has?

As reported by Henry Porter in his *Guardian* blog (25 February 2009):

> *'Once an individual has been assigned a unique index number, it is possible to accurately retrieve data across numerous databases and build a picture of that individual's life that was not authorised in the original consent for data collection,' says Sir David Omand in a report for the Institute for Public Policy Research...*
>
> *In 2006 Sir David Varney, the head of Transformational Government, predicted that the state would know 'a deep truth about the citizen based on their behaviour, experience, beliefs, needs or desires'.*

Loyalty Cards and Data-Gathering

Let's not talk about a police state, let's talk about supermarket loyalty cards. There isn't much difference between them in terms of technology, and modern ID cards seem to be close descendants of loyalty cards, intended for a similar purpose: gathering information about people. To be able to track someone, first you need to identify them.

Corporations want to know as much as they can about their customers, for marketing purposes, and have made an incredible investment in infrastructure for gathering and analysing data about them. By 2004, Wal-Mart had gathered 460 terabytes of information about customers, or more than twice the total information on the Internet.[1] The majority of this data came from loyalty cards.

Governments have adopted electronic ID cards because stores have shown what powerful and effective technology they are—not merely effective, but cost-effective. Stores have demonstrated that they can track and profile their customers to find their spending habits, their weaknesses and their suggestibility, what advertising works on them.

The technology they use not only had to prove it could work, but also had to prove it could pay for itself. If supermarket corporations invest as much as they do, the technology has to be very effective.

Powerful and effective software, such as ChoicePoint and LexisNexis, has been developed for analysing stores' loyalty card data. Now we find some of those systems in use at the FBI to shortlist suspects.[2]

Governments have realised that this same profiling technology works and can also be applied to finding terrorists, "extremists", political dissidents or any other category of interest to the state. Some of those companies also help in data-gathering.

When the US government obtained personal data about voters in 11 different Latin American states, for unspecified purposes, that data was obtained by private corporations including ChoicePoint.

It has been reported that the majority of US intelligence data-gathering is outsourced and that about 70 per cent of the budget goes to private corporations.

Although the majority of this spending goes to military-defence corporations such as SAIC and Booz Allen Hamilton, consumer corporations also take their place. So, do we see an evolving symbiosis between government and private corporations, where they share technology and tools and cooperate in data-gathering?

RFID: A Powerful Tracking Technology

One of the tools that has migrated from loyalty cards to ID cards is RFID (radio-frequency ID). It's in the new Chinese ID card and it's going into all the new "smart" ID cards.

RFID is a tracking system, originally developed to track stock in the supply chain and in warehouses. Tiny chips allow a serial number and potential other data to be read from a distance of up to several feet. When an RFID-tagged item passes a reader, its number is recorded.

When RFID readers are connected to a network, it is possible to compile a record of the movements of an object (or person) by listing the times and places when and where the RFID number was recorded.

RFID in loyalty cards allows the cardholder's name and all the personal information on the card to be read from a distance of several feet, without the cardholder's knowledge. Using RFID, stores can read your identity from your loyalty card as soon as you walk in, without your realising. Now we are being issued with government "loyalty cards" which will identify us by RFID.

The stores realised that, by placing readers at various locations, they could use RFID to track customers' movements—to see, for example, the products they looked at but did not buy, in addition to those they did.

Very quickly, the stores also realised that RFID in products such as clothing items could be used to track the movements of the people who bought them. Unlike bar codes, RFID identifies each item with a unique serial number, differentiating identical items.

The chain stores' huge databases allowed them to keep a tally of which objects had been bought by which customers—putting names to RFID serial numbers. This extra information was very powerful in "profiling" customers; for example, they started to get data about who was standing next to them, and they could guess whether customers shopped alone, with their husbands or wives, or with someone else.

Soon the stores will be able to read the RFID serial number in your national ID card in much the same way, and governments are going to sell ID confirmation to

Soon the stores will be able to read the RFID serial number in your national ID card in much the same way, and governments are going to sell ID confirmation to cross-reference the serial number on your ID card...

cross-reference the serial number on your ID card with your name and address. Stores spend a lot of money acquiring data, so knowing customers' names and addresses with certainty has really got to be worth something. Customers will no longer be able to hide their identities or give false names on loyalty cards.

When Employers Use Profiling

Some corporations already apply psychometric profiling to their staff and potential employees to get a workforce with the "right" profile, the "right" attitudes. Imagine how RFID tracking and profiling could facilitate this, profiling individuals' whole lives.

By enabling ubiquitous tracking and profiling, could ID systems herald a corporate culture of conformity, with enforced redundancy for those who don't fit the right profile?

There have been widespread examples of employers discriminating against individuals on the grounds of political or union affiliations. The UK Information Commissioner's Office found that many very large and respectable companies had engaged in illegal practices to do this.

What would happen if employers used data gleaned from ID systems and social networks analysis to profile staff, to find their friends and associates and any affiliations? What would it mean to society and political culture if corporate employers could identify and discriminate against political and union activists, making it hard for them to get a job? Would that be compatible with democracy?

RFID has an obvious application: the identities of everyone in a crowd could be collected by one mingling plain-clothes policeman with an RFID reader.

Emeritus Professor Sheldon S. Wolin, a political philosopher at Princeton University, USA, has warned of the danger of "inverted totalitarianism", as he calls it, which "lies in wielding total power without appearing to, without establishing concentration camps, or enforcing ideological uniformity, or forcibly suppressing dissident elements so long as they remain ineffectual". Such power, as in the USA, shows "how democracy can be managed without appearing to be suppressed". (Chellis Glendinning, "Every Move You Make", CounterPunch.com, 19 June 2008)

Imagine if the power of the surveillance state were applied to controlling political dissent, especially in an environment of merger between state and corporate power. Imagine dissidents being driven from their jobs or, perhaps more subtly, just denied promotion.

Imagine how detailed files on the psychological weaknesses and vulnerabilities of all individuals, generated by profiling, and records of any past indiscretions could be used to apply pressure upon opponents to government policy.

Population Surveillance and Social Control

China has become a laboratory for both capitalism and the development of new technologies for surveillance and "homeland security". Naomi Klein has written extensively about this in her book *The Shock Doctrine* (Picador, 2008) and in articles such as "China's All-Seeing Eye" and "The Olympics: Unveiling Police State 2.0" (www.naomiklein.org/articles/2008?page=1).

Some powerful people appear to have decided that capitalism works best in conditions of inequality and injustice. A by-product of this is instability: bitterness and resentment due to the appropriation of land and resources and forcing peasants off the land to become sweatshop workers living in unbearable slums.

This is about the rich getting richer by robbing ordinary people, co-opting the power of the state to do so. This is the reason for the high incidence of riots, "disturbances" and social tension in contemporary China. None of this troubles the West.

What the West has tried to do, however, is guarantee China's stability and help keep a lid on any trouble by providing China with access to the latest surveillance and security technology, to make it a more effective dictatorship. New technologies that are found to work in the social laboratory of China can be adopted and applied elsewhere.

A good example of this would be facial recognition technology, supplied to China by the US, illegally but with a nod and a wink, to make it easier for the Chinese authorities to identify troublemakers in a crowd or simply follow the movements of people of interest and perhaps identify any people whom they meet and talk with. Recognition systems now can match one face in a million, good enough to find one face in a city. How neatly this dovetails with the database of digital images provided by China's ID system.

RFID also has applications in the state security apparatus. China is issuing hand-held RFID readers to its policemen so they can take people's identities from their ID cards. It has the highest incidence of riots of any country in the world, due to the severe social conditions and inequality.

China has adopted the practice of containing disturbances rather than wading in to break them up; instead of arresting rioters on the spot, the police merely identify them—to arrest one by one at their convenience.

CCTV and surveillance technologies are used for this identification. RFID has an obvious application: the identities of everyone in a crowd could be collected by one mingling plain-clothes policeman with an RFID reader.

The RFID facility can also be useful to states with mobile populations. India is anticipating the migration of large numbers of the rural population to the cities. It plans to use a combination of RFID and GPS-based Geographical Information Systems (GIF) to automatically record the voter migration or shifting of residence and to automatically update databases such as the electoral register. One can also see how useful this would be to the Chinese authorities, with large numbers of rural peasants migrating to cities, illegally, to work as an untraceable, unstable underclass.

So, is this the model to be applied elsewhere: increasing inequality, increasing slum populations and unrest controlled through security?

Such displacement is a global phenomenon. And yes, the World Bank has an explicit role in promoting this, saying that urbanisation and migration are good and necessary things.

As described in Professor Mike Davis's book *Planet of Slums* (Verso, 2007), a huge part of the world's population lives in slums—a symptom of growing inequality and increasing exploitation. It's a trend that's ramping up.

In the USA, cities are dying, with whole neighbourhoods and in some cases whole districts being bulldozed, their inhabitants dispossessed. The plight of Detroit residents is reminiscent of post-Katrina New Orleans, with private military contractors assuming government powers in Urban Management Zones designated for wholesale clearance. This is the western manifestation of a global pattern. In 2009, the US Census Bureau plans to find even the people who have lost their homes, by employing 140,000 temporary workers to look for hidden and improvised housing units and obtain GPS coordinates for every "front door". A current legal case may make that data available to private sector corporations.

The worldwide implementation of systems for population surveillance and monitoring has to be significant. It doesn't sound like it is part of making the world a kinder, nicer place.

It's incredible how much people have willingly cooperated in handing over their personal information, cooperating in the surveillance of their lives.

What Can We Do?

We shouldn't close on such a bleak note because it simply isn't true that there is nothing we can do, although we have left it pretty late. We have a good chance if we recognise what's going wrong. We need to:

1. Organise internationally. One campaign group is slightly ahead in this area: CASPIAN (Consumers Against Surveillance, Privacy-Invasion And Numbering). It has an international membership, works closely with other groups in different nations and addresses the bigger picture, including corporate data-gathering and RFID. The author suggests CASPIAN as a good initial hub for contact.

2. Raise awareness, engage the public. It's time to raise this issue at every opportunity to get people thinking about the direction of public policy, to draw their attention to what's going on.

3. Expose the mindset of people implementing this scheme. The aim of ID cards is to create a detailed digital record of everywhere you go, everything you do. The aim of the RFID industry is Total Mobility—continuously tracking the movement of all significant objects and people. What kind of mind and personality would want such a thing?

4. Don't use cards, use cash. It's incredible how much people have willingly cooperated in handing over their personal information, cooperating in the surveillance of their lives. Try not to leave a digital record. Don't let your card identify you. ∞

Endnotes

1. Albrecht, Katherine and Liz McIntyre, *Spychips: How major corporations and government plan to track your every purchase and watch your every move with* RFID, Nelson Current, 2005, p. 64, "There's a target on your back"

2. Gellman, Barton, "The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans", *Washington Post*, 11/06/05

Editor's Note:

This is an edited version of Nathan Allonby's article "ID Cards – A World View", posted on the Global Research website on 31 August 2009. For the full text, including tables and hyperlinks, go to http://www.globalresearch.ca/index.php?context=va&aid=14992.