



Cyberlaw, Policies and Fake IDs

Internet governance and privacy policies seem to go hand in hand when issues about identity protection are raised. The scope of what we now call "Internet privacy protection" is broad, covering subjects such as digital identities, the important role of anonymity and privacy for freedom of expression, and the relationship between privacy and economic development. Several discussion groups have been formed to tackle these issues, most notably the (1) [Internet Governance Forum](#) (IGF), a United Nations conference focused on internet public policy. A big player in such discussions on internet privacy protection is the London School of Economics and Political Science Identity Project Team, the directors of the LSE Identity Project.

Let's focus on one aspect of internet government and policy: Internet technology relating to identity cards and how governments are handling this issue. The LSE Identity Project have made reports delivered in IGF conferences regarding this matter, and stated that the biometric technology, central to nationwide identification systems, has been untested at scales proposed by the UK Home Office. Online databases of the personal data of every card holder have big potentials of security attacks and information theft. Furthermore, the practicalities of implementing such a system claimed by the government and private sectors are questionable. The UK Home Office, and any government pushing for a similar National ID System for that matter, seems to be deaf against scientific expert advice, hurriedly making the conclusion in favor of their own claim: the system would work and achieve its purpose.

From the year 1939 to 1952, the United Kingdom implemented the National Registration Act 1939, wherein all citizens were required to have identity cards. This was taken as a security measure during wartime. After the war, identity cards eased up the process of rationing the supplies and goods. The scheme was similar to what is proposed today. The Identity Cards Act 2006 was given Royal Assent on the 30th of May the same year. Its main purpose also revolved around security, and it supposedly fulfills the purpose by keeping track of relevant facts about each citizen. Breaking down the broad objective of security, it aims to:

- Prevent or detect crime
- Assure that national security is maintained
- Enforce immigration controls;
- Enforce prohibitions on unauthorized working or employment; and
- Secure and maintain the public service provision

Everyone over 16 years of age is required to (2) [register their data](#) including addresses, biometric information such as fingerprints, facial measurements and iris scans. For more security, they need to visit a local centre to verify their details, facilitated by trained individuals.

Unlike the cards issued back in 1939, these new cards will have their information stored over an online database that is supposedly secure. Instead of just the military and the government having access to the data, private organizations and institutions can access them as well as long as they have been accredited. On these two points do the internet governance and policy groups extend their rebuttal. The data will be stored both in the card and on the National Identity Register, the database which is accessed via the internet. How secure really is being secure? How will they prevent unauthorized people to access information stored in the database? Can the system protect itself from information thieves who might be lurking among their own operators?

One of the risks of biometric technology is that it has not been perfected yet. It can be "spoofed" or bluffed. False biometrics can be inputted into the database. The process of spoofing is done by re-activating an underlying from a prior entry. Another method is by using a false biometric such as contact lenses just like in the Charlie's Angels movie; or using a biometric from another individual, alive or dead, like in the movies



Minority Report and 6th Day. One doesn't have to go that far to get around the system. Simple bribing might do, like the (3) "[Cash-for-fake-ID scandal](#)" where some civil servants at the Department of Work and Pensions were selling personal data to criminals to be used in making fake IDs. How would the government prevent inside jobs?

A centralized database and a uniformed ID system would definitely have its benefits, no doubt about that. But the network wherein data is accessed, inputted, deleted, and modified cannot be totally secure. There are many ways to undermine such a system, and the government has not given concrete or satisfactory proposals on how to address these issues. By just weighing the risks and benefits, people feel more insecure instead, defeating its primary goal. Privacy is everyone's friend, not all people are willing to divulge their personal data into a system that can be fooled, bribed, freely accessed and essentially lacks a secure foundation.

- (1) <http://www.csrc.lse.ac.uk/idcard/igf.htm>
- (2) <http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/103202.htm>
- (3) <http://news.independent.co.uk/uk/politics/article447792.ece>