Computers, Freedom and Privacy: The national ID debate

Report by Eugene Oscapella

SEVERAL SPEAKERS AT THE Twelfth Conference on Computers Freedom & Privacy, held in San Francisco this April, highlighted the tension between privacy and security, and in particular national security.

Among the many useful analyses of this tension was that by Andrew Schulman on the enormous technological and social hurdles to implementing national identification systems.

Schulman, a software litigation consultant associated with the Privacy Foundation, began by referring to the numerous proposals (for a national ID card) made in the aftermath of the September 11th attacks on United States. Citing the "sterile, abstract debate" that followed the attacks that suggested a slide towards greater security at the expense of privacy, Schulman noted the absence of a discussion about how a national ID card would work.

Furthermore, he asked, would it work in the context of September 11th? In other words, if a more sophisticated identification system had been in place on September 11th, would Mohammed Attah, one of the hijackers, been kept off the plane? "Frankly, if it can't do that and it is being brought up in the context of homeland security, then we don't really need to get into the privacy versus security debate - because if it is not going to work for homeland security, then why are we talking about it?"

COMPARISONS NEEDED

Schulman suggested that in considering a national identification system it made sense to first look at an existing ID programme run by the US government to assess what a national ID system for the US might look like and how effective it might be. He chose the biometric, machine-readable Border Crossing Card (BCC), a joint project of the US State Department and the US Immigration and Naturalisation Service. Schulman described the BCC as probably the largest mandatory biometric ID program run by the US federal government. About four million new BCCs, also called Laser Visas, micas, or pasaportes locales, are held by Mexican citizens, allowing them to cross into the US for up to 72 hours.

Schulman proposed a template for analysing the BCC – a template which could easily be adapted to examining proposals for comprehensive identity schemes in any country or by any business. Among the questions to be asked:

- **How are the ID cards issued?** Assuming the cards themselves are counterfeit-resistant, how easy or difficult is it to fraudulently obtain a genuine visa? What documents must be supplied when applying for the card? What background checks are performed?

- **Where are the cards checked?** Just on entry to the US? How about on exit, as part of a programme to control visa "overstays"? How is the card's 72 hour/25 mile/no work policy enforced? How much card-checking and enforcement within the US itself, away from the border, is required to secure the border? What are the penalties for violations?

- **How are the cards checked?** Are the cards visually inspected, or are they swiped through a card reader? Are the on-card biometrics being employed? How do officials verify that the cardholder and card match? Against what criminal databases is each card checked?

In his accompanying paper, Schulman warned that his analysis of the BCC gives only a hint of the complexities involved in even this relatively small biometric ID system. "It seems likely that these complexities could be magnified many times over in a National ID, to be issued to perhaps 200 million or more people."

Among the pivotal problems is the system of "breeder documents" on which a national or other form of identification document would be based. As Schulman noted, during the interview to obtain a BCC, someone must present identification documents. "To get ID, you must present ID. Documents, on the basis of which other documents are issued, are called "breeder" documents. The birth certificate is the classic breeder document... Any insecurities in birth certificates percolate up through the system."

Complicating the breeder document issue, said Schulman, is the foreign origin of many breeder documents – a Mexican birth certificate, or passport based on a birth certificate – making it even more difficult to assess their authenticity. Even US-based birth certificates may be unreliable as breeder documents. The *New York Times*, noted Schulman, has described US birth certificates as the "soft underbelly" of identification in the United States.

Even a more reliable breeder document system and counterfeit-resistant ID cards would not make the system secure, he said. The system can be subverted through bribing those responsible for issuing ID. This he described as the "insider" problem.

Schulman also reminded the audience to be sceptical of claims made by the vendors of security products. Often, he said, privacy advocates abdicate discussions of practicality to security vendors and take the vendors at their word for claims of how technology will work. (Others at the conference echoed Schulman's caution, noting that technology vendors have jumped on the national security bandwagon. As one journalist covering the event quipped, "national security is the new 'killer application' in Silicon Valley.")

Suspect secondary uses

Schulman's analysis of the complexities of identification systems highlighted other obstacles to their use, including the fear that use for one purpose (catching terrorists) would expand to other uses. "Perhaps every use to which a National ID would be put is good: keeping terrorists off planes, making deadbeat dads pay for child support, preventing underage smoking and drinking (just ask a teenager what the term "ID" means to them), making sure that gun purchasers don't have criminal records, stopping tax evasion, helping with voter registration. But the sum total of all these goods may not be what we want."

Concludes Schulman, "National ID may be a good idea or a bad idea, but the BCC experience shows us that it is a huge idea."

For further information:
www.sonic.net/~undoc/bccnew.htm;
http://www.cfp2002.org