Flawed biometrics offers false sense of security

BY DAN MCLEAN

THURSDAY, FEBRUARY 17, 2005 UPDATED AT 4:15 AM EST
SPECIAL TO THE GLOBE AND MAIL

From Britain comes disturbing news that the country's politicians seek to introduce wide-scale "biometric" identity registration for its citizens.

On Feb. 11 that nation's House of Commons passed in a 224-to-64 vote the Identity Cards Bill, which calls for the use of biometric identification cards and passports. The bill still has to clear the House of Lords, where critics say it will likely face stiff opposition, but if passed it's expected that biometric identification will go into effect by 2010 and that the documents will become compulsory for all British citizens by 2012. That could set a disturbing precedent for the rest of the world.

Biometrics, for those who don't know, involves the use of an individual's physical characteristics -- fingerprints, for example -- as identifiers. These characteristics are scanned, converted to computer code and, in the case of biometric ID cards, embedded in built-in microchips as an ID number. A card can then be matched to its rightful owner through a quick scan of the relevant body part.

Britain's Identity Cards Bill, if passed by all government levels, would mandate ID cards that include a citizen's name, address and biometric information such as fingerprints, facial scans and iris scans, according to a recent report by IDG's News Service in London. The collected data from millions of citizens would be deposited in a massive database called the National Identification Register under a plan expected to cost up to £5.5-billion ($12.8-billion).

But it's debatable why Britain sees fit to so closely track its citizens and whether folks there would even consider potentially giving up a good measure of their civil liberties in order to feel safer.

No doubt Eric Arthur Blair is rolling in his grave. Blair, better known as George Orwell, in his most famous novel *Nineteen Eighty-Four* railed against the brutal and intrusively bureaucratized governance of Big Brother in the ever-watchful fictional dystopia of Oceania. Does the ID Cards Bill have the potential to make truth both stranger and more frightening than fiction?

Aside from the disturbing potential consequences to personal freedom and privacy, the technology of biometrics, so key to the British citizen registry plan, may be more flawed than is realized by those engaged in this narrow pursuit of public safety. It's no accident that among the wide range of security technologies available, biometrics remains among the least adopted by businesses. Beyond the fact that biometric-based security is extremely costly, there are fundamental flaws in the reliability of the technology itself. That fact alone is why many banks and credit card companies don't use biometric identification systems.

In an interview reported earlier this month, for example, Johan Gerber, the associate vice-president of MasterCard International's risk products division, said that the "false positive" identification rate of biometrics is too high and the technology is simply not accurate enough. "We don't feel that it's ready to roll out just yet," he was reported as saying.

One Canadian security expert is equally skeptical. "It's pretty easy to duplicate fingerprint scans," said Kelly Kanellakis, a technologist who has worked within the security practice of a North American communications equipment manufacturer.

Fingerprints can be imprinted and "lifted" from something as simple as a soda can or duplicated with gel compounds, he explained. Iris scans are "static" or unchangeable biometric markers, which if duplicated by others become useless -- you can change a password, but you can't change your irises if someone copies a scan of them.

Likewise, security experts say a facial scan might be lifted from a photograph. And what happens as we age or when facial swelling, surgery or some other altering effect occurs? Would beards be forbidden? Perish the thought, too, that a criminal might steal a person's biometrics-based identity card and likewise feel compelled to make off with the requisite body part needed to make the thing work.

And then there's the fact that a biometric scan of a fingerprint, iris or face ultimately becomes digitized data, which although much more complex than more typical passwords and user names, is a data file nonetheless. And data can be gathered and/or decoded. Security experts suggest that ID cards with biometric information stored on them -- the so-called "smart card" -- are, from a knowledgeable criminal's standpoint, relatively simple to beat. A clever thief steals the card, strips off the biometric coding and replaces it with his own.

Those in the know say the only truly secure biometric system is one where identifiers are kept, not on millions of cards, but in a central location.

That raises yet another problem, though. Anyone with access to the central data repository where these digitized biometric scans are kept has the keys to a massive kingdom of potentially fraudulent riches. And these centralized repositories would become the primary targets of every cybercriminal type imaginable. A basic security rule-of-thumb contends that, if given enough time and enough resources, the bad guys will find a way in, so a central repository would exist as a fortress under continual and relentless siege by an ever-increasing world of marauding hacker hordes.

Consider, also, how often in recent years there have there been reports of highly confidential data from banks and governments being stolen or mysteriously going missing. It's not an unusual occurrence by any means, and suggests there may be no safe haven.

Regardless, the British government is spurred on by a perception of a dangerous and untrusting world, and forges ahead believing its measures will diminish fraud and protect the public. Proponents of the British plan to biometrically register the populace will argue that a safer society results from the use of such state-of-the-art identification and tracking.

That it is a flawed social plan underpinned by questionable security technology is closer to the truth.

Dan McLean is editor-in-chief of ITWorldCanada, a publisher of Canadian information technology magazines and on-line content. He can be reached at dmclean@itworldcanada.com