Focus
Fooling Big Brother is easier than advertised
FELIX VIKHMAN

03/15/2003
The Globe and Mail
Metro
F5

You might assume that fraudulently acquiring a fingerprint or retina for scanning would require a level of brutality most of us would rather not think about. Last year, the students of Tsutomu Matsumoto, a mathematics and cryptography professor at Japan's Yokohama National University, found a way to do it with common kitchen supplies.

Biometric devices that read fingerprints, retinas or faces are no longer the stuff of James Bond flicks. They're what increasing numbers of us have to deal with before entering the office in the morning, and soon may be a standard feature of national identity cards. So Mr. Matsumoto's question was timely: Just how secure are these security gizmos?

The Japanese class came up with a novel system that cost about $10: A perfect mould of the contours of a fingerprint was made using moulding plastic from a local hobby store. That mould was then filled with liquid gelatin, the stuff **gummy** bears are made from, available at most grocery stores. Once hardened, the gummie finger fooled commercial fingerprint scanners 80 per cent of the time (and later, presumably, made for a tasty snack).

The dozens of companies that make **biometric** devices across the world -- an estimated billion-dollar industry -- promise a world with no more keys, PINs or pass cards. Everything from high-tech government research laboratories to the information on your computer hard drive would become unreachable to nefarious intruders. Indeed, today, many laptops, handheld digital organizers and luxury car-door handles come equipped with **biometric** readers.

Recently, Immigration Minister Denis Coderre raised the idea of a "smart" national ID card that would be secured through a **biometric** imprint. Civil-liberty advocates counter that **biometric** scanners could mean a time when all individual movement could be tracked and chronicled in a central database. Steven Spielberg's future-shock blockbuster Minority Report last summer had Tom Cruise avoid retina scanners on every street corner only by resorting to an illegal eye transplant (conducted by the 22nd-century equivalent of a 1950s abortionist).

But such chilling images obscure discussion of a more here-and-now problem -- that **biometrics** may not work as promised. "The security industry has done itself a disservice by presenting **biometric** systems as a panacea," said Stephanie Caswell Schuckers, a professor at New Jersey's Clarkson University and a researcher at the FBI-affiliated Forensic Identification Research Program at West Virginia University.

Ms. Schuckers is an expert in what is called "liveness" -- detecting whether a **biometric** being scanned is actually attached to a living human being. To date, all "spoofing" techniques use an artificial implement that fools a **biometric** reader into believing it is gauging a real and living human body part. For all the high-tech, wowie-zowie appeal of **biometric** scanners, the technology to spoof them generally requires little more than a stop at a convenience store.

One method that has repeatedly been shown to work on optical fingerprint readers requires only a piece of scotch tape and a pencil lead: Apply the adhesive type to the scanner, lifting the last fingerprint to activate the device, then sprinkle crushed pencil lead on the tape. Flip the tape over, and with your own finger pressing on the back, apply tape to reader. The scanner refracts light off the pencil lead and assumes the fingerprint to be the real thing.

That trick won't deceive readers that use electronic-resonance systems, in which case **gummy** fingers prove more effective. "In our lab," said Ms. Shuckers, "we are yet to reproduce the gelatin fingers, but we have similar results using Play-doh." In any case, she added, a severed finger from a real human will always do the trick. Indeed, Ms. Schuckers has tested both electrical and optical readers with severed fingers from human cadavers

from WVU's medical school, and discovered that they spoof "universally."

Retina and face scanners are arguably even easier to spoof. What they do is convert a digital image into a mathematical algorithm, which is then matched with one in a computer database. But both systems have trouble distinguishing a real face or eye from a photographed one. Some more advanced retina and face scanners look for micro-movements to try to ensure "liveness," but a video image of person's face played on a laptop will spoof even that added level of security.

One test Ms. Schuckers is pioneering involves testing the sweat patterns of fingers. This type of fingerprint reader would test for perspiration as it collects around the edges of the finger when applied against a scanner -- sweating being something neither **gummy** nor severed fingers should be capable of. But, she admitted, "No system is perfect. People are always going to find ways around new barriers."

One way to trick **biometric** security devices wouldn't even require spoofing a human form, suggested Anil Jain, a computer-science professor and **biometrics** researcher at Michigan State University. All **biometric** security systems are necessarily hooked up to larger computer networks and databases -- and therefore susceptible to traditional computer hacking.

As well, Mr. Jain pointed out, 3 to 4 per cent of the population will always be missing the **biometric** in question. "People who work with acids and adhesives -- construction workers and cleaning ladies, say -- there is a good chance that their fingerprints are no longer of the quality that could be read by **biometric** readers."

Similarly, blind people or those suffering from glaucoma are precluded from using retina scanners. And some people, according to Mr. Jain, have nervous twitches that make it impossible for them to look at scanners for long enough to get a reading. An organization must then find other ways to identify these people, which inevitably leads to "weak security links." If Canada were to install a national ID card system, upwards of a million people would be such weak links.

Both Ms. Schuckers and Mr. Jain emphasized that the best way to ensure security, especially for something like a national ID card system, is to have actual people supervising wherever secure information is processed. "People can see what is going on, can intuitively guess if something looks wrong or if a person is acting strangely," said Mr. Jain, who pointed out that even the FBI still requires a human expert to do conclusive fingerprint matching.

"Nothing can give you the same level of security as having a human being present and aware of the situation," Ms. Schuckers agreed.

But one of the benefits often cited for national smart ID cards is that they can automate much of the communication between government and citizens. This is already the case is Spain, where people apply for social-security benefits through computerized kiosks at local malls. It helps the government save on labour costs, but it might leave the system open to tampering.

Or worse: Consider that in the future, for someone to steal your social insurance number (the basis of most of today's identity theft), they might have to cut off a finger.

Felix Vikhman is a Toronto-based writer.