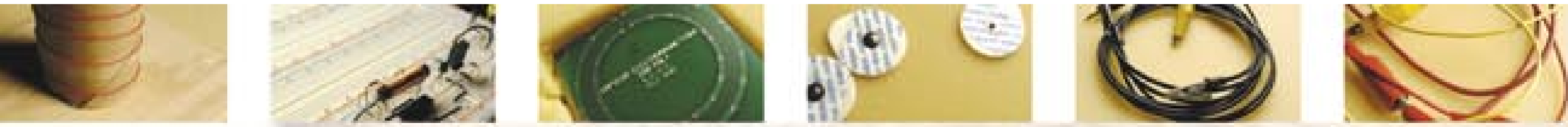
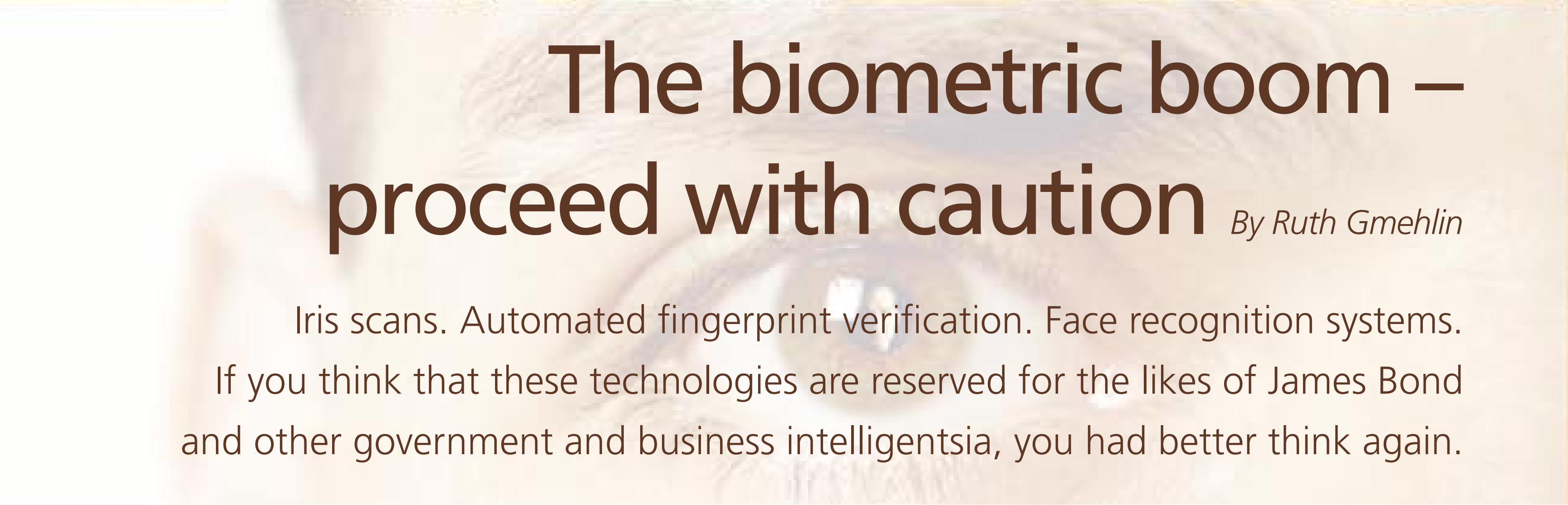
Photos by Tony Fouhse





The biometric boom – proceed with caution

By Ruth Gmehlin

Iris scans. Automated fingerprint verification. Face recognition systems. If you think that these technologies are reserved for the likes of James Bond and other government and business intelligentsia, you had better think again.

On the eve of iris-recognition technology being piloted for driver licenses and airports across Canada, the average Canadian is about to get a first-hand glimpse of the biometric future. Now the questions of security and privacy come to the fore. Are we ready to entrust, and are our governments ready to protect, this unprecedented kind of personal information?

According to Andy Adler, an assistant professor with the School of Information Technology and Engineering (SITE) at the University of Ottawa, these are the kinds of questions we should be asking as consumers.

“How much will it cost, what do we have to give up, what else could be done for the same amount of money? If you can convince me that a security measure is going to improve my life, I might be prepared to give up certain things. But I don’t want to be misled by being told I’m not giving up anything, because I know that I am.

The security industry is not selling to secret agents anymore. They are selling to people like you and me.”

Adler knows the security industry well. From 1997 to 2002, he worked for several companies in the biometrics/security arena and is now using his experience as a basis to question assumptions made by this industry.

“When I worked in the industry, I was worried about making claims about privacy and security that were unsubstantiated, things we simply had not tested or even thought out very carefully. For that reason, I really enjoy this position as a researcher. I can ask hard questions and think about them carefully.”

Adler has been busy asking hard questions. Last year, using a sophisticated computer algorithm he developed, he became the first researcher to prove that it is possible to regenerate a person’s image from a face recognition template, the supposedly non-identifiable representation of a face embedded in a bar code on an ID card.

"The assertion has been made, with almost no evidence whatsoever, that the template is a one-way transformation from an image to a bunch of 0's and 1's in a bar code, that you can't trace back and generate the original face, or thumbprint. I've shown that you can reach back into this bag of bytes and pull out your face."

The biggest implication of his work from a privacy point of view is that a biometric is essentially public information, that if you are determined, you can get somebody's picture, fingerprints or image of his or her iris.

Adler insists that while his work is not meant to hinder the industry, it does serve as a warning that consumers and vendors alike should be informed and aware of the possible limitations and pitfalls of the technology.

> "There are lots of not-so-good measures of identity floating around - no single measure is really secure."

"I think that the role of researchers like myself is to identify things that can go wrong, so that when they do, we will be more prepared to deal with them."

Not to be mistaken as an anti-biometrics person, Adler believes that well-designed and well-implemented biometrics are extremely advantageous. With the help of several NSERC grants, he is currently working on new image processing approaches to try and improve the algorithms that drive biometric recognition. He hopes that by doing so, he will be able to lower the error rates currently made by biometric machines. ■

Did you know?

- There are some people whose irises will not work with iris scanners. Some suggest that the number is as high as seven per cent. If Ontario chooses to go ahead with an iris-based driver's license, there will be a large portion of the population that won't be able to be scanned.
- The U.S. VISIT program claims that it will be able to uniquely identify anybody on the planet with the eight fingerprints it will eventually require of most foreign visitors. Most biometric experts say we don't know enough about biometric databases of more than a million people.
- While recent software is better than *some* humans at biometric matching (images to templates), about 90 per cent of people are still significantly more accurate than software.