Business

Biometrics in technology may be an easier way to ID yourself — but is it safe?

Smartphones and retailers are embracing the cutting-edge technology as an alternative to plastic cars, bar code and PINs.

CHRIS SO / TORONTO STAR FILE PHOTO

Changeroom CEO Cory Rosenfield shows a biometrically secured Nymi wristband that will notify his arrival at a retail store, alert staff to get his products ready to show and allow him to pay for them without lining up at the cash register. The Toronto-based Nymi is focused on wearable technology that identifies users based on their heartbeats.

By: Sunny Freeman Business Reporter, Published on Mon Mar 21 2016

Biometrics — measuring unique physical characteristics to verify identity — was once a form of cutting-edge technology found only in science-fiction and spy movies.

But the authentication techniques are now not only being integrated into our most-used devices, but are quickly becoming a feasible — and in some cases convenient — alternative to plastic cards, bar codes, PIN numbers and passwords.

Government and law enforcement agencies have used biometrics for years — including the century-old method of fingerprint analysis, and increasingly iris scans and facial recognition for border security and visa processing.

But many private companies in sectors from banking to health care are also embracing the technology as a personalized means of reaching potential customers, as well as a way to offer safer, more secure interactions.

The field is developing rapidly. Every smartphone, tablet and wearable device will have an embedded biometric sensor by 2020, according to Acuity Market Research. Half of purchases made on mobile devices by then will be authenticated by biometrics, according to consultancy Goode Intelligence.

Apple's Touch ID, which uses a fingerprint to unlock the iPhone, may be the best-known biometric system, but other companies are also dabbling in the space.

- Ford is exploring a biometrics system that could let users open and start their car with their fingerprints, pulse or voice, rendering keys unnecessary.
- Insurer Manulife recently launched a voice recognition system for its customers. Instead of a password, callers say "At Manulife, my voice is my password" and software determines if that matches the voice associated with an account.
- MasterCard will launch "selfie pay" in Canada later this year, letting consumers use facial recognition instead of a passcode or signature to make payments in stores. MasterCard is also testing heartbeat identification software from Toronto-based Nymi, which uses a wristband embedded with an electrocardiogram sensor.

DAVE CHIDLEY

Dr. Cheryl Forchuk has an iris scan done by associate Andrea Oni-Onafusi at her research centre in London. Forchuk is a medical researcher who is pioneering a project to see whether homeless people will agree to an iris scan as an alternative form of identification.

Retailers are interested in facial recognition software as they look for ways to target consumers when they walk into stores with products aimed specifically at them. Sales of facial recognition gear are expected to more than triple from last year's $2.8 billion to $6.2 billion by 2020, according to research firm MarketsandMarkets.

Companies would love to be able to use the technology to reduce shoppers to a unique consumer profile, but they can't move faster than people are comfortable with, said Andy Adler, a professor of systems and computer engineering at Carleton University.

"It's still a dream of being able to narrow down uniquely," he said.

Although the technology has made strides, widespread adoption is still hindered both by consumer reluctance and unreliability.

Even if biometrics is more secure than a chip or PIN, using it is still in many cases an inconvenience. To employ biometrics, retailers would have to purchase terminals and consumers would have to deal with the glitches and delays that come with cutting-edge technology.

"Companies would prefer to lose one per cent of their income in fraud and stop annoying customers with fingerprints and face recognition and everything else," said Adler.

Fingerprints, faces and iris scanning are still the most-developed forms of biometric identification. But even those systems have limitations and can be fooled. Consider bad lighting. Or your smile. That's why you have to look grim in your passport photo — the detection software doesn't work with varied facial expressions.

Fingerprinting is probably the most widely known type of biometric ID, but it is also one of the most easily copied or "spoofed."

When Brazilian banks rolled out fingerprint-reading ATMs to stamp out fraud, criminals simply severed the fingers off of account holders to access their money. A Chinese woman escaped detection when entering Japan by getting her prints surgically altered, while a Dominican doctor was convicted for offering to surgically alter fingerprints of illegal aliens in the U.S.

SANDER KONING

A man uses a smartphone with an app that allows online payments using biometric authentication, an emerging type of technology that may remove the need for plastic cards or PINs while shopping.

Similar methods of spoofing — using printed images and the like — have also fooled facial recognition and iris scanning software.

Meanwhile, Adler believes voice recognition, gait measuring or ear-shape analysis are still too new to be trusted on their own — at least to the degree needed for widespread adoption.

“They’re exciting, but we’re not going to see uptake until they start working well,” Adler said. “Things haven’t changed as much as one might guess.”

But the field may still be advancing quicker than some are comfortable with.

Facebook is fending off allegations that it “secretly amassed the world’s largest privately held database of consumer biometric data” in a lawsuit over its photo-tagging tool.

That wariness on the part of consumers about giving up identifying data to big corporations is one of the main hindrances to wider spread adoption, said Karl Martin, founder and chief technology officer at Nymi.

That’s why his company is focused on wearable technology that identifies users based on their heartbeats. All data is stored locally in the device and users always have the option to take it off, at which point it is deactivated, he said.

“Privacy is not so much about keeping things secret, but about the user being in control of their information,” he said.

People are growing increasingly comfortable with biometrics, such as using wearables to track health data or using their fingerprints to unlock their phones, but there are still many questions over where data is being stored and managed and by whom, he said.

“The world is ready for biometrics, but there are still people and companies that are trying to do it in a way that could be dangerous,” said Martin. “That’s something I think we should all be wary about.”