

# Digitizing you

## Identifying who's who in a virtual world

by Marlene Orton

**As recently as April 16, CTV NewsNet talked about the billions of dollars that Canadian governments at all levels are forecasted to spend on increased security, and how American firms, engaging the interest and confidence of public sector buyers, hope to capture a share of that money. But a young Canadian biometric industry – working virtually underground for the last few years – is rising to meet the challenge for new security solutions in Canada and abroad in the aftermath of last September's terrorist attack. The science and technology of creating and identifying the unique digital "signature" of a part of the human body is becoming big business.**

The North American market for biometric technology is expected to reach US\$2.6 billion by 2006, although it is uncertain how much of that figure involves security expenditure. Regardless, millions of dollars' worth of contracts are at stake as the governments of Canada and the United States, as well as those of other G7 industrialized countries, implement measures for enhanced airport security, pre-approved border clearance, passport ID verification and permanent resident smart cards.

Close to home, new security initiatives outlined in the Canada-US Smart Border Declaration ([www.can-am.gc.ca](http://www.can-am.gc.ca)) and signed December 12, 2001, pledge joint development "on an urgent basis" of common biometric identifiers built into smart cards and other documents. Market opportunities for biometric identification extend to the European Union and to larger global requirements through the International Civil Aviation Authority, headquartered in Montreal.

The Canadian Biometric Group ([www.cata.ca/biometrics](http://www.cata.ca/biometrics)), under the wing of the CATA Alliance in Ottawa, was formed in mid-January – months ahead of its planned launch – in response to the September terrorist attacks. The Group moved quickly on several fronts to coalesce a fragmented industry, disseminate information on biometric technology, strengthen ties with Industry Canada and, in turn, begin the task of introducing industry members to the government network.

"Our mandate is to promote the Canadian industry across the country and give them a platform," says Peter Turpin, executive director of the Canadian Biometric Group. "So I guess [that means] digging in and looking at what Industry Canada has and what other avenues are available, such as working with the embassies, and anybody who is interested in biometrics, and trying to provide the information flow to the membership so they can grow their business on a global basis and in Canada."

Barely a month after the Canadian Biometric Group appeared, John Siedlarz, chair of the US-based International Biometric Industries Association, was in Ottawa at a speaking engagement. Siedlarz, a co-founder of Iridian Technologies (focusing on iris biometrics), now serves on the advisory board of the Canadian Biometric Group.

Canadian biometric companies have spent several years honing their technology and have established a toe-hold in the US and overseas in the UK and Germany. The Ottawa Telephony Group (OTG), which builds software applications around a voice-verification biometric, provides the US Senate in Washington with voice verification to secure PBX resources. Overseas, the UK National Crime Squad is using biometric facial-recognition software developed by Imagis Technologies Inc. of Vancouver ([www.imagistechnologies.com](http://www.imagistechnologies.com)). In Germany, the Bundesdruckerei Gruppe purchased rights to sell a facial-recog-

nition biometric advanced camera and software security system developed by Ottawa's BioDentity System Corporation ([www.biodentity.com](http://www.biodentity.com)) to speed security processing at European Union airports and border crossings.

Now these and other Canadian biometrics companies have emerged from virtual stealth mode to face a dual challenge:

- target and educate the Canadian government and law enforcement agencies with proven Canadian capability; and
- learn the ropes of defence and security procurement at home.

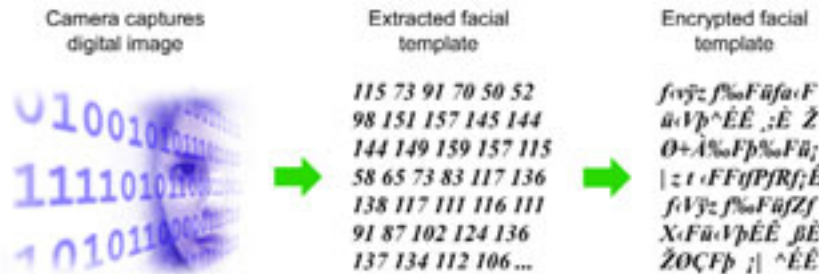
Despite the horrific events of September 11, the timing could not have been more precipitous for the biometric industry. Government and police agencies almost immediately called for tenders on border security and public safety systems. Outstanding Request For Proposals (RFP) and planned security measures were modified.

Canada Customs and Revenue Agency (CCRA) quickly released an RFP for an iris scan biometric-based Expedited Passenger Processing system for frequent air travellers between Canada and the US. Deputy Prime Minister John Manley announced the Canadian passport would soon include a biometric identifier.

The RCMP modified its approach to procuring a Real Time Identification system with a revised procurement strategy to meet new federal security policies. In mid-March, four British Columbia RCMP detachments purchased a new Computerized Arrest and Booking System from Imagis Technologies Inc. based on biometric facial recognition software for speedier forensic lineup ID.

NEXUS, the cross-border pilot jointly run by CCRA, Citizenship and Immigration Canada, US Customs Service and US Immigration and Naturalization Services, began in late 2000 at the Sarnia, Ontario/Port Huron,

## How it works



Pete Harroff, VisionsSphere Technologies Inc.

Michigan border crossing as a bilateral Customs Action Plan. The pilot at the Blue Water Bridge used proximity card technology on the US side, and photo ID cards and licence plate reader technology on the Canadian side.

NEXUS was suspended after September 11 but was reinstated and vastly expanded in late 2001 as part of the Canada-US Smart Border Declaration Action Plan ([www.ccra-](http://www.ccra-ardc.gc.ca)

With surprising speed, the Government of Canada launched a biometric/security showcase in late March at the Canadian Embassy in Washington.

"I have tried to run one or two technology seminars a year on a hot topic or a topic of great interest to the US," says Richard Malloy, business development trade officer for defence, aerospace and technology at the embas-

# A biometric is something that you are

[ardc.gc.ca](http://www.ardc.gc.ca)). The enhanced NEXUS will use a biometric identifier. CCRA spokeswoman Colette Gentes-Hawn says the RFP for a fingerprint biometric was to be issued on the US side.

Across several Canadian government departments, antennae were quickly tuned to intelligence signals from the biometric community.

"We are constantly on the lookout for capability and we keep pulling information in and shopping it around through Foreign Affairs and International Trade," says Jamie Hum, director of Industry Canada's Information and Communication Technology Branch. "That's been in place for a while and it seems to work very well. Our mandate is to identify and promote the Canadian capability in different areas like security. The Canadian Commercial Corporation (CCC) is also an important organization. We refer companies to the CCC ([www.ccc.ca](http://www.ccc.ca)) so they can specifically understand how to qualify for US defence procurement."

sy. "In this post 9/11 environment, because security has been so heightened, I was looking for something by which Canada could assist the US in the area of security. Biometric is one of those areas, and there may be others out there. I may be planning a whole series of these seminars starting in the new fiscal year."

Some 300 invitations were sent to US government personnel, welcoming members of the Department of Defense (DoD), the State Department, Department of Commerce, and law enforcement agencies, as well as other organizations, to attend.

"Everyone thinks of the US federal government but sometimes some of the key players are actually the US prime contractors and they heavily populate my guest lists," Malloy says. He also relied on the Biometrics Group and Industry Canada for Canadian corporate invitations. Individual biometric companies that have secured contracts in the US helped provide information on key US players, he adds. The biometric showcase was not an exclusive event, however.

## Solutions with vision



- Sales
- Rentals
- Installations
- Service
- Creative Services
- Communication Seminars

### duocom

Canada's Leader in Presentation Solutions

[www.duocom.ca](http://www.duocom.ca)

888-338-6266  
(Bilingual)

## Understanding biometrics

Only a year ago, biometrics was mainly regarded as an adjunct security feature in e-commerce, with growing use in the United States for document authentication in driver's licences and resident cards. Things changed. "Obviously with the security concerns that came up in September, all of a sudden companies looking at this from the viewpoint of e-commerce saw an application in different terms," explains Jamie Hum, director of Industry Canada's Information and Communication Technology Branch.

The term biometrics suggests a late 21st century technology, but it was coined more than a century ago. Sir Francis Galton's fingerprint biometric – based on statistical analysis of unique human whorls and ridges – has been used in law enforcement for nearly a century. His analytical method dating to the 1890s was refined and is still largely used today in Great Britain and throughout North America. A disciple of Galton was British scientist Karl Pearson, whose interests included statistical analysis of biology. Pearson called this science biometrics.

Today, analysis of distinct human biological traits extends to facial recognition, voice verification, iris scans, hand geometry, even vein patterns at the wrist. But the enabling technology of the late 20th century has permitted wide exploitation on a scale the pioneering British mathematicians could never have dreamed.

The processing power of modern computers has enabled high-speed computation with faster complex tabulations resulting in biometric comparisons produced from a database of tens of thousands of samples in just a few seconds. It can take a single facial image and using algorithms – a model that reduces complex information to a simpler mathematical expression – match it with the identical model in a huge database.

Typically in biometrics, a person provides a sample of a fingerprint, facial image or iris. This is scanned electronically, processed and stored as a template. Unique features are segregated, coded then encrypted and registered in a database. Contrary to TV forensic dramas, photographic images are not overlaid for a match. Digital codes are matched.

Verification or authentication is confirmed by matching on a one-to-one basis. John Q. Smith's identity is verified by matching his print against John Q. Smith's original template. In a one-against-many search, a person's biometric is enrolled and matched against the database to identify a person as John Q. Smith.

A biometric is frequently considered a third layer of security. "A password and a PIN is something you know," says Peter Turpin, executive director of the Canadian Biometric Group of the CATA Alliance. "A swipe card or proximity card is something that you have. A biometric is something that you are."

"If any biometric firm (was) unable to come, I will be more than happy to help, to advise, to guide at any time they want to get in touch with me or come down and visit me. The assistance I give to Canadian industry is not limited to two seminars a year," says Malloy.

In Ottawa, Canadian Police Research Centre (CPRC) also sponsored a showcase at the National Research Council in late February to preview a trial BlueBear Network, aimed at providing a high-speed national police network of mug shots. BlueBear uses Vision-Sphere's face-recognition software and includes major high-technology partners such as Dell Computers Canada, Microsoft Canada, and Texar Corp.

CPRC ([www.cprc.org](http://www.cprc.org)) is a partnership between the Canadian Association of Chiefs of Police, RCMP and the National Research Council (NRC). Its objectives include forging

partnerships with Canadian industry and providing "technology partner" evaluation to Canadian police and government agencies, security firms, and industry. Companies benefit by testing capable technologies under operational conditions, giving them credibility to compete domestically and internationally.

Equally important are CPRC's connections. Showcase attendees included municipal and federal law enforcement authorities, the US Department of Justice and federal Office of the Solicitor General. Both the embassy and NRC showcases served as informal RFIs (Requests for Information), a useful venue particularly with an emerging technology. This venue is more common among UN agencies, especially International Civil Aviation Organization (ICAO) whose New Technologies Working Group (NTWG) is responsible for researching, analyzing and reporting new technologies in aviation security.

During ICAO's ([www.icao.int](http://www.icao.int)) high-level Ministerial Conference on Aviation Security in mid-February, NTWG invited RFIs and demonstrations from several Canadian biometric companies. ICAO's Doc 9303 Technical Advisory Group for Machine Readable Travel Documents or MRTDs, under which NTWG falls, will require member states to enhance passport and other documents with a biometric identifier.

"ICAO is trying to develop an approach supported by specifications so that no matter where you travel in the world, a single biometric would be globally interoperable," says Joel Shaw, BioDentity's CEO and president. "It is a very important requirement. If you can reach an agreement worldwide on a standard biometric for global interoperability, it would put that particular biometric in a unique position."

International standards, even uniform national standards, for biometrics technologies are not yet fully developed. CPRC evaluations are an important means of establishing performance criteria.

However, the US DoD has already taken the initiative with a Biometrics Fusion Center, set up to allow industry, government and university researchers to work together to establish standards. As well, DoD has had Executive Agent for Biometrics with a Biometrics Management Office ([www.c3i.osd.mil/biometrics](http://www.c3i.osd.mil/biometrics)) in place since late 1999 under the auspices of the US Army. Guides to vendors and other certification expectation are available online.

Canada's biometric expertise is gradually stretching globally. The US-based Biometrics Consortium ([www.biometrics.org](http://www.biometrics.org)), with activities in standards development, trade-shows and conferences, now includes several Canadian companies.

Among them is OTG ([www.otg.ca](http://www.otg.ca)). "We are not visible simply because we are in an area that people didn't believe in, to start off with," says OTG president Mark Kovalsky. "Trying to sell a biometric five years ago was like swimming upstream in a heavy current." ❧

---

*Marlene Orton is a freelance writer based in the Ottawa area.*