Information and Privacy Commissioner/Ontario
Commissaire à l'information et à la protection de la vie privée/Ontario

News Release **March 14, 2007**

New Privacy-Enhancing Biometric Technology: Biometric Encryption promises superior privacy, security, and personal control over biometric data

TORONTO – The Information and Privacy Commissioner of Ontario, Ann Cavoukian, Ph.D., and Alex Stoianov, Ph.D., an internationally-recognized biometrics scientist, today announced the publication of their joint research paper, *Biometric Encryption: A Positive Sum Technology that Achieves Strong Authentication, Security AND Privacy,* available at www.ipc.on.ca .

Biometrics are unique physiological characteristics of an individual, such as a fingerprint or iris scan, that can be used to recognize and verify their identity. As the use of biometric technologies become more widespread, so does the risk to individual privacy. The creation, growth and data linkage of biometric databases may enable new forms of surveillance, profiling, discrimination, and identity theft. While widespread adoption of biometric technologies is on the horizon, it should not come at the cost of personal privacy.

"Biometric data – fingerprints, DNA, or irises – are unique identifiers," says Commissioner Cavoukian, "far superior to social insurance numbers in that they are a unique and permanent characteristic of individuals. This makes biometric data a very powerful tool for matching different pieces of information held about individuals across multiple databases."

Further, Commissioner Cavoukian adds that, "Biometric data can also serve as a password in that it can be used to gain access to physical spaces (restricted areas) or to electronic systems (databases). The security risks of large centralized databases of biometric passwords cannot be underestimated, and unlike passwords, biometric data is permanent – you cannot change your fingerprints or irises if your biometric data is lost or stolen."

Fortunately, biometrics *can* be deployed in a privacy-enhanced way that minimizes the potential for surveillance and abuse, maximizes individual control, and ensures full functionality of the systems in which biometrics are used. Building privacy-enhancing technologies into biometric-enabled systems will also create greater confidence in those systems, leading organizations and the public to place greater trust in their use.

Our white paper sets out the privacy, security and trust problems of current biometric information systems, and explains how an emerging new technology, called Biometric Encryption, can address those concerns.

With Biometric Encryption (BE), instead of storing a sample of one's fingerprint in a database, you can use the fingerprint to encrypt or code some other information, like a PIN or account number, or cryptographic key, and only store the biometrically encrypted code, not the biometric itself. This removes the need for public or private sector organizations to collect and store actual biometric images in their database.

… /2

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
http://www.ipc.on.ca

Thus, most privacy and security concerns associated with the creation of centralized databases are eliminated. BE allows an individual's biometric data to be transformed into multiple and varied identifiers for different purposes, so that these identifiers cannot be correlated with one another. Better still, if a biometric identifier is somehow compromised, a completely new one may be easily generated from the same finger or iris of an individual.

BE also promises other exciting new possibilities which are discussed at length in the paper. One such possibility is the creation of anonymous databases. Another possibility is the promise of enabling individuals to use their biometric identification for direct and secure access to their own files. Still another possibility is to place strong and easy-to-use encryption capabilities at the fingertips of millions of individuals, without the need to literally memorize any passwords, PINs, or carry around physical pass-keys.

BE technology not only holds the promise of superior privacy and personal control for individuals over their own biometric data, but also stronger information security and greater user confidence and trust in biometric identification systems.

With the publication of this paper, we are encouraging the public, policymakers, information security professionals and technologists everywhere to examine Biometric Encryption, with its numerous privacy and security advantages, and to consider its adoption and deployment as a privacy and security-enhancing alternative. We also wish to inform the public that there are more preferable alternatives to the existing privacy-invasive security technologies (zero-sum, win/lose) currently being deployed by government and businesses – positive sum (win/win) alternatives which can deliver both privacy and security. User confidence and trust in the privacy and security assurances of any information system that relies upon biometrics will be critical to the acceptance, use and ultimate success of that system.

ABOUT THE AUTHORS

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world and the published author of two groundbreaking books on privacy – *Who Knows: Safeguarding Your Privacy in a Networked World* (1997), written with Don Tapscott, and *The Privacy Payoff: How Successful Businesses Build Customer Trust* (2002), written with Tyler Hamilton. Overseeing the operations of the freedom of information and privacy laws in Canada's most populous province, Commissioner Cavoukian serves as an Officer of the Legislature, independent of the government of the day.

Alex Stoianov, Ph.D.
Dr. Alex Stoianov began working in the field of biometrics after joining Mytec Technologies Inc. (Toronto, Canada) in 1994, where he was one of the originators of the privacy-enhancing technology, Biometric Encryption. Working for Bioscrypt Inc., the successor of Mytec, as a Principal Scientist from 2001 to 2006, he developed numerous technological breakthroughs and improvements for fingerprint verification algorithms. He also won the Third International Fingerprint Verification Competition (FVC2004), viewed by many as the "Fingerprint Olympics," on the company's behalf. Dr. Stoianov has co-authored more than 30 scientific papers and 7 patents.

Media contact:
Jason Papadimos
Communications Co-ordinator
Office of the Information and Privacy Commissioner of Ontario
Desk: 416-326-8828
Cell: 647-408-5556
jason.papadimos@ipc.on.ca