Biometric Encryption: A Positive Sum Technology that Achieves Strong Authentication, Security AND Privacy

Executive Summary

The Information and Privacy Commissioner of Ontario, Ann Cavoukian, Ph.D., and Biometrics Scientist, Alex Stoianov, Ph.D., jointly released a white paper entitled *Biometric Encryption: A Positive Sum Technology that Achieves Strong Authentication, Security AND Privacy*. The authors wish to appeal to a broader audience in considering the merits of Biometric Encryption (BE) to verify identity, protect privacy, and ensure security. Their central message is that BE technology can help to overcome the prevailing "zero-sum" mentality involved with traditional biometrics, namely, that adding privacy to identification and information systems weakens security. This need not be the case. They believe you can have both privacy and security: you do not have to choose one over the other.

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. Biometric technologies promise to enhance the effectiveness of identification and authentication processes, help control access to physical and electronic resources, and improve the security of information systems. However, done poorly, biometric technologies can be highly privacy-invasive. Biometric data, once collected, can be stored, shared and used for numerous secondary purposes, inviting potential discrimination and identity theft.

While widespread adoption of biometric technologies is on the horizon, the authors believe that it should not come at the cost of personal privacy. This paper illustrates that biometrics may be deployed in a privacy-enhancing manner that minimizes the potential for surveillance, maximizes individual control, and ensures full functionality of the systems involved. Building privacy-enhancing technologies into biometric-enabled systems will also allow the public to place greater trust in their use.

With Biometric Encryption, instead of storing a sample of one's fingerprint in a database, you 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. Thus, most privacy and security concerns associated with the creation of centralized databases are eliminated.

A positive-sum model, in the form of Biometric Encryption, presents distinct advantages to both security and privacy. The paper provides three case studies that exemplify how Biometric Encryption is applicable to small, medium and large scale applications. It outlines the advantages of BE over other biometric systems as being: 1) no retention of the biometric image or template, 2) multiple, revocable identifiers, 3) improved authentication security from stronger binding of user biometric and identifier, 4) improved security of personal data and communications, 5) greater public confidence, acceptance, and use, 6) greater compliance with privacy laws and, 7) suitability for large-scale applications.

In acknowledging that research in BE has been on-going since the 1990s, the authors set out the issues that need to be addressed as the next phase for Biometric Encryption (creation and testing of a prototype) fast approaches.

By publishing this paper, the authors wish to advance current national and international discussions regarding the most appropriate and privacy-enhancing methods by which to achieve strong identification and authentication protocols. They strongly believe that privacy must not be not be forfeited in one's search for greater security – you can have both.