Biometric Identification and Privacy Concerns: A Canadian Perspective

AIRD & BERLIS LLP
Barristers and Solicitors

By Paige Backman and Corrine Kennedy

Biometrics – An Introduction

Biometric identification, or the use of unique physical or behavioural characteristics to identify individuals, is often viewed as the stuff of which movies are made. However, identification from biometrics, which stems from the Greek *bio* ("**life**") and *metric* ("**measurement**"), has been around in the real world for years in various forms.

Biometric identification or authentication has traditionally been based on human processes: a person comparing characteristics of an individual to those characteristics of individuals that have been otherwise obtained. Examples include the comparison of drivers' license photos to the person presenting it, the use of signature cards by banks and the comparison of fingerprints in the context of criminal investigations.

Advancements in technology have greatly expanded the types of biometric information that we are readily able to collect from individuals, as well as the ways in which such biometric information can be used. Facial structure, fingerprints, speech patterns, voice recognition, iris composition and retinal scans, gait, hand geometry, vein pattern and even body odour are a few examples of biometric identifiers. The purposes for which biometric data may be used to identify or authenticate an individual may be broadly divided into four categories: (i) to permit physical access to restricted areas; (ii) to confirm an entitlement to services;[1] (iii) to monitor or record certain facts;[2] and (iv) to associate a particular activity with an individual.

Unlike passwords and other traditional measures used to secure information or prevent access, biometric information cannot be forgotten or misplaced by the individuals using it. This notion, coupled with the fact that biometric information is ultimately personal in nature, largely unchangeable and distinctive from individual to individual, has resulted in a widespread belief that biometrics is ideal for identification or authentication purposes.

However, the characteristics which make its use ideal for the purposes of identification or authentication are the same characteristics which raise concern among privacy advocates. These concerns center around the high risks associated with the wrongful disclosure, theft or misuse of biometric information. The severe consequences of these risks require the biometrics industry and the private and public sector working with biometric technologies, to not only strictly adhere to existing privacy legislation,[3] but also to examine and work with government authorities to revise regulatory frameworks to ensure this highly sensitive information is adequately protected from misuse and theft.

Compliance with Canadian Privacy Legislation and Biometric Data

The collection of unique and unchangeable information about individuals, its storage (both in Canada and internationally) and its use (as intended and for secondary purposes) have fuelled discussion about how Canadian privacy laws should be applied to biometrics and the technologies surrounding its use.

The *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**")[4] is Canada's federal private sector privacy statute. It regulates the collection, use and disclosure of personal information in the private sector for all commercial activities involving cross-border flows of personal information, and the flow of such personal information within all of Canada's provinces except British Columbia, Alberta and Quebec. British Columbia, Alberta and Quebec each has its own private sector privacy legislation regulating the flow of personal information within provincial borders.[5]

Canadian privacy laws at the federal and provincial levels are largely based on what is colloquially referred to as fair

information handling practices. There are several key elements which make up the fair information handling practices that underpin Canadian privacy laws: (i) informed consent, (ii) reasoned and limited collection, use and disclosure of personal information; and (iii) ensuring such personal information is adequately secured. Organizations must be open about their purpose for collecting personal information[6] and obtain informed consent before collecting, using or disclosing the information.[7] Further, companies are obligated to destroy, erase or make anonymous personal information no longer required to fulfill the purpose for which it was collected.

These fair information handling practices constitute the general standards governing the collection, use and disclosure of personal information. Guidance surrounding specific compliance obligations are developed through the "findings" and "rulings" of various privacy commissioners across Canada.

The application of Canada's privacy laws to biometric data is no different than the application of privacy laws to any other type of personal information. To this end, the Privacy Commissioner of Canada (the "Privacy Commissioner") has applied PIPEDA's provisions in several contexts. In one instance, the Privacy Commissioner examined the collection by an employer of employee voice recordings, which were to be used to replace passwords to authenticate the employee's use of business applications while off-site.[8] In another instance, the Privacy Commissioner investigated the Law School Admission Council's collection of fingerprints from students taking the Law School Admissions Test.[9]

In both instances, the Privacy Commissioner applied the test found under subsection 5(3) of PIPEDA, which evaluates the appropriateness of the purpose expressed for collecting the personal, in this case biometric, information. The test asks the following four questions: (i) is the measure demonstrably necessary to meet a specific need; (ii) is it likely to be effective in meeting that need; (iii) is the loss of privacy proportional to the benefit gained; and (iv) is there a less privacy-invasive way of achieving the same end?[10] It is important to note that even if the collection, use and disclosure of biometric information meets this test, consent of the individual from whom the biometric information is collected is still required, except in the specific instances outlined under PIPEDA.[11]

These cases demonstrate that the use of biometric data is not *prima facie* problematic in Canadian privacy laws. If collected and protected correctly, using advanced and secure technologies, biometrics may lead to better identification than current password or cardholder-based protection systems. Unlike a password, which is easily forgotten, or an access card, which can be lost or stolen, you carry your biometric data with you wherever you go and, in theory, only you would be able to produce your own biometric data for authentication purposes.

However, since the fair information handling practices are fairly general and illustrated through fact-driven scenarios detailed in "findings" and "rulings," companies are left to apply the fair information handling practices to their own business processes, rather than having concrete guidance and rules enumerated under Canadian privacy legislation. In the face of new technologies, application of general principles by companies into unchartered territory, including new types of biometric data and the use of related technologies, can be challenging. This may mean that companies are reticent to move in new directions of better and more secure biometric technology. As discussed below, a loyalty to the use of traditional and existing biometric technologies and traditional approaches to the collection, use and disclosure of biometric data under the current forms of privacy legislation may leave the personal information of individuals vulnerable to privacy breaches. A breach involving biometric data can have very significant consequences that are not easily rectified.

Concerns about Security, Theft and Misuse of Biometrics Data

What makes biometrics so useful is also what makes it so essential that privacy legislation requires companies to adhere to high and specific standards for its protection. Biometric information is unique to each individual and remains relatively unchangeable. Accordingly, if a security breach results in the theft of biometric information of one individual or thousands, managing the risk of harm to such individual or individuals is not as simple as cancelling a credit card or changing a password.

Accordingly, privacy commissioners and advocates have begun to examine different processes for collecting, storing and using biometric data. Biometric identification or authentication often uses a "one-to-many" comparison, meaning that the information is compared to others in a larger database of information to find a match.[12] For the purposes of this type of comparison, biometric identification involves the collection of information from one individual. The biometric information (in the form of data, a biometric template or image) is attached to a specified individual and is stored in Canada or elsewhere in the world. This stored information becomes a unique identifier for that individual. The storage of biometric information on large pools of individuals, where unique and intensely personal identifiers are linked directly to various individuals within that pool, does not lend itself to ensuring the privacy and security of the individual's personal information, and raises concerns about the misuse or secondary use of the biometric data being stored.

What if the biometric information was untraceable to an individual? Ensuring the information could not be re-engineered to access the individual's stored profile, data or captured biometric image would offset many of the concerns surrounding the security and misuse of the personal information, while maintaining the integrity of this seemingly ideal form of identification.

The Ontario Privacy Commissioner, Ann Cavoukian, (the "**Ontario Commissioner**") has discussed the development of "Untraceable Biometrics." In theory, untraceable biometric technologies are secure technologies, enabling the processing and use of biometric information in a manner which does not associate the biometric data to an identifiable individual because it does not store biometric images or a biometric template. The original biometric data cannot be recreated from the stored information. In ways that vary from technology to technology, the biometric data submitted by an individual is irreversibly and untraceably converted into an otherwise unrelated data string, personal identification number (PIN) or key. Once the individual re-presents the biometric information, the unique PIN or key is recreated and compared with the string that has been stored. Essentially, the biometrics may be seen as a decoder of the unique PIN, allowing the individual to be authenticated.[13]

This technology often uses a "one-to-one" approach (meaning that the information is about one individual, is stored, and ultimately compared with a live sample provided by one individual) which allows for control of biometric information to rest with the individual to whom it belongs.[14] It cannot be worked backward to access biometric information about an individual, and can be revoked or cancelled if the system is compromised.[15] Accordingly, even if the system were to suffer a privacy breach, the individual's data would remain secure.[16] Advancements in the field of untraceable biometric technology have moved the use of biometrics much closer to this incorruptible ideal.

Though such untraceable biometric technology exists, it is rarely used. The Ontario Privacy Commissioner has identified various reasons, particularly in the public sector, for the sparse use of this newer technology. In part, the reliance on the traditional collection and storage of traceable biometric information results from the newness of the more advanced technology. More advanced untraceable biometric technologies are unfamiliar and less understood, tend to be unsuitable for application in every context, and, as with many new technologies, may appear prohibitively expensive to businesses evaluating their security needs and attempting to meet the minimum privacy compliance threshold required by law.

We note as well that infrequent use of biometric technologies means that they remain fairly untested, in respect of the application of 'fair information handling practices' in the "findings" and "rulings" made pursuant to applicable privacy legislation. Accordingly, companies subject to privacy legislation, whether federal or provincial, may be hesitant to move in this newer direction without more concrete standards and guidance.[17]

Conclusion

The use of biometric information and the development of biometric systems to process such personal information are still relatively new and continuously being analyzed, reviewed, and modified. As this technology develops and changes, as does the kinds of biometric information being collected, used and disclosed, it will undoubtedly be further scrutinized for accuracy and efficiency.

In theory, the use of biometric data for identification or authentication purposes is ideal. However, the broad principles upon which Canadian privacy legislation are based, with general standards for compliance coming in piecemeal form, largely through "findings" and "rulings," render the current existing privacy regulatory framework inappropriate. Accordingly, companies are left to implement privacy legislation in a significant vacuum of direction and concrete compliance requirements.

There are various arguments in favour of leaving the determination of detailed standards relating to the collection, use, disclosure and security of biometric data to the organizations handling such data. Some arguments are more persuasive than others. In part, the general standards on which Canadian privacy laws are based allow for flexibility in adapting to new technologies. However, this flexibility also means that, with each new technology and each new type of personal information collected or used, organizations are left to determine, within the framework of broad principles forming the basis of Canadian privacy laws, what is 'reasonable' and what is not.

Practitioners working with privacy compliance issues are all too aware that decisions by companies about what security measures and privacy practices to implement for the protection of personal information are largely determined by the present tangible costs companies will incur, particularly in a tight economy. Given the personal and unchangeable nature of biometric data, coupled with the fundamental problems that can arise from its misuse or theft, leaving issues such as requisite security measures to individual organizations is unacceptable. Rather, Canadian privacy legislation must be adapted and reworked to change with the technology, provide concrete guidance to companies subject to its provisions,

and ensure that the biometric information of Canadians remains adequately protected.

Paige Backman is a partner at A&B in the Corporate/Commercial Group and Technology Team. Paige may be reached at 416.865.7700 and pbackman@airdberlis.com. Corrine Kennedy is an associate with A&B's Corporate/Commercial Group and Technology Team. Corrine may be reached at 416.865.7709 and ckennedy@airdberlis.com. Deep appreciation is extended to Karen Levin and Shanika Shaw, summer students at A&B, for assisting with various elements in the preparation of this article.

---

1 For example, NEXUS is a biometric-based system that expedites border crossings between Canada and the United States by allowing low-risk passengers (who are members of the program) to authenticate themselves through the use of retina and thumbprint scans.

2 Examples include the monitoring of employee attendance or the retrieval of banking or health records. This type of biometric system has already been the subject of national attention in Canada, in the form of biometric sign-in systems for employees. An Edmonton nightclub implemented a thumbprint-scanning computer device to track the arrival and departure times of its employees. See the *Edmonton Journal*, "Employee thumbprint scanners used at Edmonton club ruled legal," *The Vancouver Sun* (3 September 2008), online: Canada.com http://www.vancouversun.com/index.html.

3 It is important to note that, in Canada, the federal public sector is governed by the federal Privacy Act, R.S.C. 1985, c. P-21 ["***Privacy Act***"]. The *Privacy Act* may not provide protection as extensive as that found in PIPEDA in respect of biometrics, as it limits the definition of "personal information" to information that is "recorded in any form." Biometric data, then, is only protected by the *Privacy Act* if it has been recorded in some form (e.g. if it had been converted into written data or stored as a recorded image). Accordingly, as discussed later in this paper, traditional methods of storing biometric data as images may be captured by the *Privacy Act*, but newer Untraceable Biometrics, as defined herein, may not be contemplated by this wording. The Office of the Privacy Commissioner of Canada has recently recommended that the Privacy Act be amended, stating that unrecorded information "can yield intelligible information about identifiable individuals [and] [a]s such, it should have legal protection." (See *Parliamentary Activities: Privacy Act Reform* (29 April 2008) online: Office of the Privacy Commissioner of Canada http://www.priv.gc.ca/parl/2008/parl_080429_02_e.cfm#rec7.

4 S.C. 2000, c. 5 [PIPEDA].

5 See Alberta's *Personal Information Protection Act*, S.A. 2003, P-6.5 [PIPA]; British Columbia's *Personal Information Protection Act*, S.B.C. 2003, c. 63 [B.C. PIPA]; and Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. c. P-39.1. Several investigations and cases in each jurisdiction have examined the use of biometrics, whether collected in respect of customers or employees. In Alberta, an Edmonton nightclub required its employees to scan their thumbprints into biometric scanning systems, but the nightclub did not inform the employees how the technology worked and how it collected information. Although the Alberta Information and Privacy Commissioner (the "Commissioner") determined that the scanning system was not an invasion of privacy, the Commissioner found that the nightclub had not properly complied with paragraphs 15(2)(c) and 18(2)(c) of PIPA. These sections place a duty on organizations to specify what personal information is being collected and used in addition to the purpose for the activity. See *Empire Ballroom (1208558 Alberta Ltd.)*; *Investigation Report P2008-IR-005* (27 August 2008), online: Office of the Information and Privacy Commissioner of Alberta http://www.oipc.ab.ca/pages/home/default.aspx. In another Alberta case, privacy concerns were raised with the Commissioner after a nightclub employee had scanned the complainant's driver's licence information into a database without his consent in order to enter the establishment. Rather than verify his age, the scanner had taken a digital picture of his licence, and the picture was automatically stored in a "SecureClub ID System." The Commissioner held that the nightclub had failed to comply with the requirements of subsections 11(1) or 11(2) of PIPA, and concluded that the collection of such personal information was not reasonably related to the nightclub's purpose. See *Order P2006-011*; *Penny Lane Entertainment Ltd., Penny Lane Entertainment Group, Tantra Night Club Inc. (Re)*, [2008] A.I.P.C.D. No. 49 (QL), leave to appear refused: [2009] A.J. No. 300 (Q.B.) (QL).

6 *Supra* note 5, Schedule 1, s. 4.2.

7 *Ibid.*, at s. 4.3.

8 See PIPEDA Case Summary #2004-281. This case was also considered by the Federal Court of Canada, when a section 14 application was brought under PIPEDA in respect of the same matter.

9 See PIPEDA Case Summary #2008-389.

10 *Ibid.*, at par. 46.

11 For the exceptions to the consent requirements, see PIPEDA subsection 7(1).

12 Ann Cavoukian and Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (March 2007), at 5-7. ["***Biometric Encryption***"]

13 Ann Cavoukian and Max Snijder, *A Discussion of Biometrics for Authentication Purposes: The Relevance of Untraceable Biometrics and Biometric Encryption* (July 2009), p. 1, available online: Information and Privacy Commissioner of Ontario http://www.ipc.on.ca/images/Resources/untraceable-be.pdf, at 1. ["***A Discussion of Biometrics***"]

14 *Supra*, note 13.

15 *Ibid*.

16 A Discussion of Biometrics, p. 2-3.

17 The Ontario Privacy Commissioner has also suggested that privacy advocates and the Canadian public as a whole have not applied sufficient pressure in requiring the use of this more secure biometric technology from the public and private sectors. For discussion of these and other reasons that Untraceable Biometrics has been used less often, see Biometric Encryption, p. 11. Also, see recent information released by Citizenship and Immigration Canada on its pilot biometrics project for temporary residents entering Canada, which requires a photographic image and the enrolment of ten fingerprints before arrival in Canada, to be compared with the individual's biometric information on arrival. See Citizenship and Immigration Canada, "Temporary Resident Biometrics Project," available online at http://www.cic.gc.ca/english/department/media/backgrounders/2009/2009-06/18.asp.