National Banking Law Review

General Editors: Blair Keefe and Eli Monas, Torys LLP

VOLUME 34, NUMBER 3 Cited as 34 Nat. B.L. Rev. JUNE 2015

• 2015 FEDERAL BUDGET – FINANCIAL SERVICES HIGHLIGHTS •

Dawn Jetten, Elizabeth Sale, and Vladimir Shatiryan
Blake, Cassels & Graydon LLP

• In This Issue •

Finance Minister Joe Oliver tabled his first budget on April 21, 2015 (the "Budget"). Several proposals in the Budget will be of interest to financial institutions, including proposals for a consumer protection framework for banks, expanding the voluntary mortgage prepayment commitment to non-banks, a national financial literacy strategy, a bank recapitalization framework, regulation of retail payment networks, and access to basic remittance services.

Consumer Protection Framework for Banks

The government proposes a new financial consumer protection framework for banks that will provide:

- Broadened general requirements for clear and simple disclosure of information, and expanded use of summary information boxes for banking products and services. There were no details on which additional products and services will require summary information boxes. Currently, information boxes are required for consumer loans and prepaid payment

products, suggesting that information boxes may be required for optional products and services, deposit accounts, registered products, and deposit-type instruments. Banks will be required to revise impacted documents and processes in order to comply with additional information box requirements. Aside from new summary information box requirements, there was no indication as to which additional general requirements for clear and simple disclosure may be required and how this will enhance the current requirements to provide disclosure that is clear, simple, and not misleading.

- Improved access to basic banking services by allowing a broader range of personal identification to open an account. This proposal is limited to basic banking services and we expect it will be aligned with existing identity verification requirements under anti-money laundering laws and anticipated changes to those requirements.
- Expanded prohibitions on certain business practices, including high pressure sales situations, and cooling-off periods for a greater range of products. No guidance was provided as to which business practices would be prohibited. We note that there is currently a prohibition against tied selling that refers to imposing undue pressure or coercing a person. Presumably, any new prohibitions would be outside of the tied selling context and would only apply where fees or other charges are payable. Regarding cooling-off periods, while the Budget did not specify which products would be affected, it included an example about savings accounts. Implementing and tracking cooling-off periods will add yet another layer of development and cost for banks.
- Expanded corporate governance requirements so that boards of directors' duties relate to all consumer protection measures. This will close a perceived gap in the duties now prescribed under the *Bank Act*.[1] Currently, the directors' specific duties relating to consumer protection are limited to (1) establishing procedures to provide required disclosures to bank customers and for complaints handling; and (2) establishing procedures to resolve conflicts of interest, including techniques for the identification of potential conflict situations and restricting the use of confidential information, which is not limited to consumer-customers but does relate to the protection of personal information.
- Improved transparency and accountability, for example through enhanced public reporting on complaints and on measures taken to address the challenges faced by vulnerable Canadians. Banks will be required to provide public reports on an annual basis demonstrating how their business activities meet the spirit of the consumer protection principles to be set out in the *Bank Act*.
- A requirement that advertising be clear and accurate. It is not clear how this would enhance or supplement the existing prohibitions against false and misleading advertising set out in the *Competition Act*.[2] Perhaps the goal is to extend the existing requirements that certain prescribed disclosures be made in a language and presented in a manner that is clear, simple, and not misleading.

The framework will be achieved by consolidating the existing consumer protection provisions in the *Bank Act*, which will be anchored by a set of principles (to be set out in the *Bank Act*) to guide bank conduct. At this stage, it remains to be seen to what extent the consumer provisions under both the *Bank Act* and its regulations will

be consolidated — which could eliminate duplication and unintended differences in the current multiplicity of regulations — and the extent to which such consolidation will include changes to the consumer provisions beyond those highlighted in the Budget. A key provision in these announcements will be the definition of consumer. The government has not indicated whether this will be limited to natural persons acting for a purpose other than that of carrying on business. The framework will be overseen by the Financial Consumer Agency of Canada.

The Budget states that in creating the framework, the government is delivering on its commitment in Economic Action Plan 2013 ("the 2013 budget") to implement a comprehensive financial consumer code. The government is also proposing to make amendments to the *Bank Act* intended to address the Supreme Court of Canada's decisions in the *Marcotte*[3] cases. This proposal builds on the government's efforts to ensure that banks should only be required to comply with federal consumer protection laws (and not provincial consumer protection laws). For example, the government intends that the financial consumer framework be *comprehensive* and the *Bank Act* provide the *exclusive* set of rules governing consumer protection for banks. In 2012, the government added the preamble to the *Bank Act* with similar language and intent; however, this did not sway the Supreme Court of Canada in the *Marcotte* cases. It remains to be seen whether the proposed new amendments to the *Bank Act* will have the desired effect. The Budget states that the government will continue to engage with provinces and territories. If such engagement includes discussions on *Marcotte*, and the provinces and territories agree with the government's position, this would be a very positive development for banks.

Expanding the Voluntary Mortgage Prepayment Disclosure Commitment

The Budget states that the government will invite all mortgage lenders to agree to provide enhanced information about prepaying mortgages, similar to the voluntary commitment made by the banks to this effect. As it would appear that the invitation will be extended to *all* mortgage lenders, we anticipate that the government will be engaging with not only other federally regulated mortgage lenders such as federal trust and loan companies, insurance companies, and the retail association, but with provincially regulated mortgage lenders as well.

Financial Literacy Strategy

Building on its strategy to enhance the financial literacy of seniors, the government will be releasing a national strategy for Canadians of all ages, in co-ordination with the Financial Literacy Leader. The Budget highlights the commitment from Canada's banks to establish a five-year Financial Literacy Partnership Fund of $10 million to provide grants to eligible community organizations for projects that work to improve the financial literacy capabilities of Canadians.

Bank Recapitalization (or "Bail-In") Framework

The government reiterated its intention to introduce a new bank recapitalization (or "bail-in") regime for Canada's six largest banks, which have been designated by the Office of the Superintendent of Financial Institutions ("OSFI") as domestic systemically important banks ("D-SIBs"). Originally announced in an August 2014 Consultation Paper, the proposed bail-in

regime will introduce a new statutory conversion power authorizing the government to convert a D-SIB's long-term unsecured liabilities into common shares in the event of non-viability of the D-SIB. The government confirmed that only unsecured liabilities that are tradable and transferable, and have an original term to maturity of 400 days or more will be subject to the statutory conversion. Deposit liabilities will be exempt, and liabilities issued and not renegotiated before the implementation date will be grandfathered. The proposed new statutory conversion power will supplement the existing non-viability contingency capital requirement that applies to all federal deposit-taking institutions and requires the conversion of non-core capital instruments, such as preferred shares and subordinated debt, into common shares on the non-viability of the institution.

The government confirmed that a new minimum loss-absorbency requirement will be introduced for D-SIBs. According to the August 2014 Consultation Paper, this would be a new capital measure that D-SIBs must meet through the sum of their regulatory capital and bail-in eligible senior unsecured debt. The recent international consultations by the Financial Stability Board on the Adequacy of Loss-Absorbing Capacity of Global Systemically Important Banks in Resolution are expected to inform the government's approach to developing this new capital measure.

The government will also introduce legislative amendments to the *Canada Deposit Insurance Corporation Act*[4] provisions governing the resolution and recovery of banks in Canada, together with associated regulations and guidelines. Although the August 2014 Consultation Paper suggested that a holding-company structure could be introduced for D-SIBs, the government clarified in the Budget that no holding-company requirement will apply to Canadian banks as part of the changes to bank resolution and recovery laws.

Reinforcing the Housing Finance Framework

The government proposes to implement regulatory measures that limit the extension of portfolio insurance through the substitution of mortgages in insured pools, tie the use of portfolio insurance to Canada Mortgage and Housing Corporation ("CMHC") securitization vehicles, and prohibit the use of government-backed insured mortgages as collateral in securitization vehicles that are not sponsored by CMHC. The government included a substantially similar proposal in Economic Action Plan 2013 and, as before, there are no details on how such proposals will be implemented. This is all part of the efforts of the government to limit consumer debt — particularly mortgage debt — and limit government exposure to the housing market.

Financial Sector Oversight

The government proposes to modernize, clarify, and enhance the protection of prescribed supervisory information that relates to federally regulated financial institutions. Confidentiality of information exchanged with supervisors is essential to ensuring fulsome disclosure. The current legislation has proven to be insufficient to maintain the intended confidentiality and too restrictive with respect to circumstances in which supervisory information may properly be shared.

Credit Unions

The government indicated that it will continue working with stakeholders on the implementation of the federal credit union framework and

the transition of provincial credit union centrals out of OSFI's federal oversight.

Regulation of Retail Payment Systems

The Budget makes reference to a new consultation on the oversight of Canada's retail payment systems, which was announced earlier last week. The Consultation Paper, entitled *Balancing Oversight and Innovation in the Ways We Pay*, considers how Canada's retail payment systems should be regulated. The proposed government oversight would apply to "national retail payment systems", the scope of which is not fully defined: it would include major debit and credit card networks that are national or substantially national in scope, and could extend to other providers of payment services, such as telecommunications and Internet companies offering payment services.

It is proposed that national retail payment systems would be regulated in three respects: operational risk, market conduct, and efficiency in the retail payments sector. The regulation of operational risk would target management of risk by the payment systems, as well as measures to ensure data security, user privacy, and safeguarding of user funds. However, no specific proposals have been introduced so far.

The market conduct regulation would ensure end-user protection, which must be consistent across all payment systems. In this respect, the Consultation Paper seeks comments on whether the current reliance on voluntary codes — including the recently amended *Code of Conduct for the Credit and Debit Card Industry in Canada* — should be supplemented by legislation. A mandatory registration or licensing of payment service providers is also raised as an option, which, if implemented, would presumably be independent from the current registration requirement for money services businesses under the anti-money laundering legislation. In addition, the Consultation Paper seeks comments on whether the rules of the Canadian Payments Association should be extended to "on-us" payments by financial institutions (where payments are made between two customers of the same financial institution).

Regulation of efficiency in the retail payments sector would aim at discouraging abuse of market power by prominent retail payments systems and encourage adoption of technical standards facilitating inter-operability of domestic and international payments systems.

The consultation period ended on June 5, 2015.

Ensuring Canadians Have Access to Safe, Reliable and Lower-Cost Remittance Services

The government proposes measures to help ensure Canadians have access to safe, reliable and lower-cost remittance services when sending money to developing countries. As part of these measures, the Budget proposes the development of a remittance price comparison website that will provide information on fees charged across service providers. The government suggests that it will work with financial institutions to evaluate possible options to expand access to lower-cost remittance services. These measures would likely impose ongoing reporting requirements on providers of remittance services and may have an impact on the price of such services, in particular if the intent is to require providers to offer a basic, low-cost service option. It is not clear why or how these initiatives would focus on remittances to developing countries only.

Modernizing Canada's Corporate Governance Framework

The government proposes amendments to the *Canada Business Corporations Act* [*CBCA*][5] relating to gender diversity, director elections, shareholder communications, and corporate transparency. The Budget states that amendments to related statutes governing co-operatives and not-for-profit corporations will also be introduced to ensure continued alignment among federal laws. Notably, the Budget does not include mention of the *Bank Act*, *Trust and Loan Companies Act*,[6] or the *Insurance Companies Act*,[7] even though such statutes' corporate governance frameworks are modelled off the *CBCA*.

[*Editor's note:* **Dawn Jetten** is co-chair of the Financial Services Regulatory Group at Blakes. She has extensive experience providing advice to numerous Canadian and foreign financial institutions, including banks, trust companies, loan companies, insurance companies, commercial and consumer finance companies, and a variety of other financial service providers.

Elizabeth Sale is an associate in the Financial Services Regulatory Group at Blakes. Her practice focuses on the regulation of financial institutions and other financial services providers, including banks, foreign banks, captive finance companies, payday lenders, insurance companies, trust companies, loan companies, and participants in the payment card industry.

Vladimir Shatiryan is an associate in the Financial Services Regulatory Group at Blakes. His practice focuses on a broad range of issues impacting Canadian and foreign financial institutions.]

---

1 S.C. 1991, c. 46.
2 R.S.C. 1985, c. C-34.
3 *Bank of Montreal v. Marcotte*, [2014] S.C.J. No. 55, 2014 SCC 55, [2014] 2 SCR 725; *Marcotte v. Fédération des caisses Desjardins du Québec*, [2014] S.C.J. No. 57, 2014 SCC 57, [2014] 2 SCR 805; *Amex Bank of Canada v. Adams*, [2014] S.C.J. No. 56, 2014 SCC 56, [2014] 2 SCR 787.
4 R.S.C. 1985, c. C-3.
5 R.S.C. 1985, c. C-44.
6 S.C. 1991, c. 45.
7 S.C. 1991, c. 47.

• BANKING AT THE TIP OF YOUR FINGERS: PRIVACY CONSIDERATIONS SURROUNDING BIOMETRIC IDENTIFICATION AND AUTHENTICATION IN FINANCIAL SERVICES •

Molly Reynolds, Eliot Che, and Lara Guest
Torys LLP

Canadian and global industries are adopting new biometric technologies at an unprecedented rate. New smartphones now often come equipped with fingerprint sensor technology,[1] and software will implement facial and iris recognition technology into future Windows 10 devices. This trend is just as present in the financial industry.[2]

Financial institutions, both in Canada and abroad, continue to develop or deploy fingerprint, voice and electrocardiographic recognition systems for the identification and authentication of banking customers. The implement-tation of biometric technologies into consumer banking systems may assist in preventing fraud or identity theft.

However, the inherently personal nature of biometric information may also increase the risk to privacy interests in such forms of data. Accordingly, the emerging use of these new technologies raises an important question: Is the current Canadian privacy framework equipped to deal with the collection, use, and storage of biometric information?

This article presents an overview of biometric identification and authentication, and its current uses both within Canada and internationally, followed by an assessment of the current privacy law and security landscape surrounding the implementation of biometric technologies.

What Is Biometric Identification?

Biometrics is the study and measurement of biological data. Biometric identification is the process of identifying individuals through the analysis of unique physical or behavioral characteristics. For example, biometric authentication systems may identify individuals using their fingerprints, finger or palm vein patterns, iris or retina markings, voice patterns, facial features, heartbeat, gait, or biodynamics (such as the speed and pace of an individual's typing).[3]

Unlike alphanumeric passwords and personal identification numbers ("PINs"), biometric data is inherently personal and generally immutable. The personal nature of this information has advantages for identification and authentication purposes — an individual cannot forget her fingerprints. Therefore, biometric information is by and large considered a reliable source of data that is not easily replicated. However, the personal and immutable nature of the information creates significant privacy and security concerns when collecting, storing, and using biometric data — the misuse or theft of biometric information may have severe consequences.

Existing and Evolving Uses of Biometrics

Biometric identification is not new. For decades authorities have identified drivers by comparing their faces to their drivers' license photograph, financial institutions have identified clients through the use of signature cards, and police have apprehended suspects after dusting a crime scene for fingerprints.

Although the concept of biometric identification is not innovative, our increasingly digital economy is facilitating new forms and increased availability of such measures. Contemporary technological advancements are expanding the types of biometric information that can be measured, the capacity to collect and store the information, and the potential uses for such data.

Biometrics in Canada. Canadian financial institutions are now developing and deploying systems that draw on fingerprints, voice recognition, and electrocardiography to identify clients and authenticate their credentials.

Fingerprint authentication was recently introduced by the Bank of Nova Scotia for Tangerine banking clients. Complementing the traditional password, customers are able to log into the Tangerine mobile banking app using their fingerprints (for example, using the fingerprint identity sensor built into recent Apple iPhone devices).[4]

Voice recognition is employed by TD Waterhouse to identify clients using telephone banking services. Rather than asking personal questions such as birth date and postal code to verify an individual's identity, a client's voice acts to provide her with "instant access".[5] Tangerine also uses voice-based banking — customers are authenticated through their voice patterns after answering a series of questions.

Electrocardiographic authentication for the financial sector is currently being developed in a joint pilot project by Royal Bank of Canada and MasterCard. In simple terms, the client's heartbeat serves as his authenticating password for credit card payments at point of sale terminals. A wearable wrist device reads the heart's electric activity — the client then places her wrist over an existing point-of-sale system (such as MasterCard's Paypass Tap & Go or VISA's payWave) in lieu of a credit card to authorize a transaction.[6]

Biometrics internationally. Financial institutions outside Canada are similarly deploying a wide range of biometric technologies in consumer banking services. In 2008, Cairo Amman Bank became the first in the world to install iris recognition systems at branches and ATM locations in Palestine and Jordan.

In the United Kingdom, finger vein authentication is available to Barclays business customers. Finger vein patterns are considered a reliable source of biometric information, as they remain stable throughout an individual's life. When near-infrared light is transmitted through a finger, part of the light is absorbed by the hemoglobin in the veins. The patterns generated by the light absorption are unique and can be used for authentication.[7] Finger or palm vein authentication is also used widely in Poland and Japan. In Poland, thousands of cash machines have been installed that permit customers to access their accounts by scanning their fingers instead of using cards or PINs.[8]

Privacy Issues in Biometrics

In part because more rudimentary forms of biometric identification have been in place for decades, and in part because Canada's Office of the Privacy Commissioner ("OPC") is closely monitoring developments in biometric technology, the deployment of the above banking tools is unlikely to require a sea change from a privacy law perspective. In many ways Canada's existing privacy law framework is well-equipped to deal with emerging uses of biometric identification. Similar to other modern identification systems such as PINs and signature cards, biometric identification may involve the collection, use, disclosure, and storage of personal information. Existing legislation and jurisprudence provide extensive guidance on privacy complaint information handling practices, which may apply broadly to the collection and use of biometric data from consumers by financial institutions.

However, certain new technologies may present risks not yet anticipated or addressed in the existing privacy framework. A breach involving biometric data stored by a financial institution can have significant consequences, which may not be easily rectified using current approaches to identify theft protection and compensation for economic harm. A security breach involving a PIN is serious, but a PIN can be changed — a breach involving fingerprint data cannot be rectified in the same manner and the data could be misused in manners beyond those typically guarded against in privacy breach responses.

The Existing Privacy Legislation Framework

The *Personal Information Protection and Electronic Documents Act* [*PIPEDA*][9] regulates the flow of personal information in the private sector across Canada, with the exception of Alberta, British Columbia, Quebec and Manitoba. These four provinces have separate yet substantially similar private sector privacy legislation regulating personal information within their borders.

There are three key elements underlying Canadian privacy legislation:

- informed consent;
- reasoned and limited collection, use, and disclosure of personal information; and
- adequate safeguards for personal information.[10]

Organizations must disclose the purpose for collecting personal information and obtain informed consent before doing so. Informed consent must be obtained before an organization can use or disclose an individual's personal information. Companies are also required to destroy, or anonymize, personal information that is no longer required for its stated purpose.

The OPC recognizes that biometrics "can serve as the foundation for robust and reliable identification systems";[11] however, the OPC notes that not all biometric characteristics possess equal degrees of uniqueness: "Many biometric characteristics, for instance, can be highly distinctive, with little or no overlap between individuals. Fingerprints, irises and DNA are among the most distinctive characteristics, while facial features may be more similar among different people."[12]

Recognizing that different biometric data may share risks similar to conventional personal information and have other risks that are distinct, the OPC has recommended a privacy impact assessment methodology specifically directed at biometrics and has published several findings following complaint-triggered investigations involving the use of biometrics.

Privacy Impact Assessments

The OPC recommends that a Privacy Impact Assessment be completed before launching new programs involving biometrics, although they are mandatory only for the public sector institutions under the *Privacy Act*.[13] For example, the OPC has worked with Passport Canada over several years to address the privacy implications of biometric-based electronic passports. The key considerations were restricting data stored on chips in passports, securing the information, ensuring proper disposal, and avoiding centralized databases of the biometric information collected.[14]

The position of the OPC is that the authentication system must be designed to provide the least information necessary to achieve the justifiable purposes of the system.[15] In assessing privacy implications of any new system, the OPC uses a four-step test adopted from *R. v. Oakes*:[16]

Is the measure demonstrably necessary to meet a specific need? The OPC suggests that a biometric system should not be adopted simply because it appears to be the most convenient or cost-effective option — organizations should identify both the specific problem and why biometric data is essential in order to satisfy this need.

Is it likely to be effective in meeting the need? Effectiveness likely depends on the nature of the biometric data. For example, while facial recognition systems are widely used in identification documents such as passports and drivers' licenses, facial features can be altered and thus may not be sufficient in authentication contexts requiring a high degree of certainty.

Is the loss of privacy proportionate to the benefit? There will necessarily be some loss of privacy in a biometric identification system. The analysis of whether the benefits granted by the system will outweigh the loss of privacy may depend on the biometric characteristics employed. Some forms of biometric data are more

privacy-sensitive than others. For example, fingerprints are a particularly sensitive form of biometric data, and the benefits to the proposed system must therefore be greater if the organization intends to use a fingerprint identification system.

Is there a less privacy-invasive means of achieving the benefit? The OPC suggests that organizations ask whether there may be a less privacy-invasive way of achieving the same result. For example, facial recognition or smart cards may achieve the same benefits as other types of biometric data, such as fingerprint scanning, without affecting privacy to the same degree as other technologies.

Decisions of the OPC are reflective of this approach, including *PIPEDA Case Summary No. 2011-012*,[17] which concerned the authentication of Graduate Management Admission Test ("GMAT") test-takers using palm vein scanning technology. The complainant objected to having her palm scanned before writing the 2009 GMAT, and also objected to the disclosure of her biometric information to an American organization. The biometric system converted the vein pattern into an encrypted numerical template. No actual biometric data was retained in a record that could be readily deciphered.

The OPC concluded that a reasonable person would consider the use of palm-vein scanning appropriate in these circumstances after considering the factors above. First, test administrators had provided the OPC with evidence of professional test-takers, some of whom had written the GMAT hundreds of times on behalf of other individuals. Second, palm-vein scanning was demonstrated to be effective at both deterrence and detection of fraud. The biometric technology was shown to be effective as a deterrent against fraud and impersonation during examinations of this nature, and the test administrators demonstrated the success of the palm-vein scanning technology in detecting test-takers using counterfeit government identification. Third, the technology was not overly invasive, since palm-vein data was not considered overly sensitive personal information. Further, the palm-vein scans were immediately transformed into an encrypted binary template. The biometric identification process could not be reversed and the binary code information could not be easily interpreted by third parties. Fourth, the biometric information was encrypted, and data access was restricted. The encryption algorithm was a "recognized encryption standard with good security levels for sensitive data" and the data was also protected by multiple safeguards at the data storage centre. For example, the documented security policies, written agreements with third-party contractors, and a data retention period of five years satisfied *PIPEDA* principles with respect to safeguarding personal information.

Privacy Concerns in Collecting, Verifying and Storing Biometric Data

The OPC has provided recommendations for each step of the biometric authentication process, including

- data collection;
- verification methods; and
- data storage.

Data Collection

The OPC recommends minimizing the amount of data collected. For example, organizations may elect to record summary information only, where possible — essentially extracting a portion of the biometric information to record

a "template" or mathematical summary of the data. The OPC notes that "where a business or government agency doesn't really need to know the individual's identity, but merely that the individual is authorized to do something (use a credit card) or entitled to receive something (a government benefit), individuals can protect their privacy by restricting the identifying information that they surrender about themselves".[18]

Proprietary extraction methods can be used to limit the ability to use templates collected for one purpose to be used for another purpose. Such methods include cancellable biometrics, biometric tokens, and biometric encryption. Cancellable biometrics involves distorting collected biometric data through the insertion of random bits of data that can only be isolated using auxiliary data such as a password (sometimes called "hashing" or "salting"). Biometric tokens may include, for example, stand-alone devices or apps such as numeric token generators that work in conjunction with biometric data. These methods are biometric examples of the two-factor authentication techniques increasingly in use throughout the financial services industry, and more broadly. Biometric encryption involves one-way cryptography, described further with regards to verification below.

Verification Methods

There are two main methods of verifying biometric data: "one-to-many" and "one-to-one".[19]

In a "one-to-many" comparison, an individual's credentials are verified by comparing her information to the biometric information of others located within a larger database to find a match.[20] For the purposes of this type of comparison, biometric identification involves the collection of information from one individual. The biometric information is attached to a specified individual and is stored in a central database. The storage of biometric information of 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. One-to-many verification methods raise concerns about the misuse or secondary use of stored biometric data.

In contrast, a one-to-one verification procedure does not require the comparison of an individual's biometric information against a broader biometric database. "Untraceable Biometrics" is one form of one-to-one technology, and has been examined by the Information and Privacy Commissioner of Ontario. Untraceable biometric technologies are secure technologies that allow an individual to be identified through the use of biometric information without associating the information to the individual. The biometric data submitted by an individual is converted into a data string. When the individual presents his or her biometric information, the data string is recreated, and compared directly to the data string stored. Essentially, "the biometrics may be seen as a decoder of the unique PIN, allowing the individual to be authenticated".[21] This one-way processing of biometric data is largely considered to be preferable from a privacy perspective as the biometric data cannot be recreated from the stored information.

Data Storage

Local storage is preferable to a centralized database, since centralized systems are more likely to be subjected to hacking, potentially resulting in large scale data breaches.[22] Local storage can be achieved through the use of smartcards, or

storage of the biometric information directly on the device hardware.

Although the OPC places significant emphasis on encryption and other technical security safeguards for biometric information, once data is collected there is always the possibility that it may be accessed or used for purposes not disclosed to the individual (either lawfully, such as by way of subpoena for records relevant to litigation, or unlawfully, such as by targeted hacking).[23] As a result, organizations should develop comprehensive security and privacy policies to minimize the potential unauthorized use or disclosure, as well as implement information request policies and breach response plans.

Specific Concerns with Facial Recognition Technologies

The OPC has noted that facial recognition technology has the potential to be highly invasive, since the facial information can, from a technical standpoint, be collected without an individual's consent or knowledge.[24] The OPC distinguishes between voluntary programs involving facial recognition from those involving covert collection. For example, the use of facial recognition software on individuals entering a casino who have voluntarily asked to be placed on a no-gambling list is not an unjustifiably intrusive biometric identification system.

In contrast, social networking sites that use facial recognition technology on user-uploaded photos may be engaged in more covert practices. The OPC has pointed to Facebook as possibly the world's largest database of images that can easily be associated with other personal information on individuals' profiles, and the use of facial recognition in smartphone security. Similarly, the OPC has identified the growing use of facial recognition technology on mobile devices, which scan a user's face and unlock the device if it matches an image previously stored by the user.[25]

Canada has not adopted any official standards for the protection of privacy in the context of biometric information. Although the current privacy framework is generally applicable to biometric technology, and the federal and provincial privacy commissioners have provided some insight in this area, the lack of standards specifically targeting biometric technologies leaves financial institutions with some degree of uncertainty regarding the implementation of adequate privacy protections.

Although international standards may be applied by analogy to perceived gaps in the Canadian framework governing privacy and biometric technology, these standards have yet to be applied consistently in the financial industry or formally approved by domestic privacy authorities.

Other Risks

Security concerns

Significant data security risks are associated with the collection and storage of personal biometric information, including theft and fraud using improperly obtained information, both of which may result from techniques such as hacking. While there are currently no Canadian security standards governing the storage of biometric data, international standards may provide guidance to financial institutions seeking to protect information in their possession.

Theft

All data stored digitally is at risk of theft, particularly data stored on network-connected devices. Biometric identification systems suffer from vulnerabilities similar to that of databases

of credit card numbers. There, as with other forms of personal information, both physical security measures, software and hardware based security methods, and securities policies are required to secure the storage of biometric data.

Recent data breaches at retailers such as Home Depot and Target highlight the risks in the electronic storage of personal information. The Home Depot data breach resulted in the theft or exposure of approximately 56 million credit and debit card numbers including other personal information, while the Target data breach involved approximately 40 million credit and debit card numbers. However, affected customers were able to have their credit cards re-issued with new numbers. Because of the general immutability of biometric information, stricter security guidelines and techniques may be required. For example, storage of biometric information locally, on the user's hardware instead of on the company's network, may assist in preventing widespread theft of customer biometric information. This method is used by Apple in its deployment of fingerprint readers on recent models of the iPhone.

Fraud

Similar to other identification systems, both electronic and non-electronic, biometric identification systems are also at risk of fraud. For example, German hacker "Starbug" recently demonstrated the vulnerability of biometric identification systems during an unofficial crowdsourced competition.[26] According to the BBC, he "hacked Apple's Touch ID a day after its launch, replicating the last fingerprint that had touched the glass iPhone surface with … a scanner, a printer and a bit of glue". The hacker was also able to recreate a fingerprint from photographs taken from ten feet away.

The German hacker advocates for a "two-factor" identification system whereby two of the following three different types of authentication are required: knowledge-based, such as a password; possession-based, such as smart cards; and biometrics, such as fingerprints. Increasing the methods of identification associated with access, while potentially more cumbersome, help protect the identification process from fraud.

International Security Standards

The FIDO ("Fast Identity Online") Alliance is a non-profit organization formed in July 2012 to address both the lack of interoperability among strong authentication devices as well as the difficulties users face in creating and remembering multiple usernames and passwords. The FIDO Alliance's standard for security devices and browser plugins will allow any website or cloud application to interface with a broad variety of existing and future FIDO-enabled devices possessed by the user for online security.[27] In February 2014, Samsung and PayPal announced a collaboration that enables Samsung Galaxy S5 users to complete mobile payments using a fingerprint sensor and software that has been certified by the FIDO Alliance.[28]

The International Organization for Standardization ("ISO") also provides security guidelines for the storage of biometric information.[29] The ISO is an international standard-setting body composed of representatives from various national standards organizations.[30] The ISO standard for biometric information provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during transfer and storage. ISO Subcommittee 37 focuses on the standardization of generic biometric technologies to support interoperability and

data interchange between biometric systems and applications. For example, the standards suggest common file formats, biometric templates, and application programming interfaces.

Outsourcing Standards and Emerging Issues

The Office of the Superintendent of Financial Institutions ("OSFI") prescribes outsourcing requirements applicable to many institutions under its supervision in Guideline B-10: *Outsourcing of Business Activities, Functions and Processes* ("Guideline B-10"). However, OSFI's expectations with respect to outsourcing arrangements may extend beyond compliance with the provisions of Guideline B-10.

Financial institutions that deploy biometric identification and authentication technologies involving third party service providers should have regard to the process for assessing the risk and materiality of outsourcing arrangements set out in Guideline B-10. Generally, Guideline B-10 holds the financial institution ultimately accountable for all outsourced activities. The guidelines also require the organization to document all material outsourcing arrangements in written contracts. As noted above, biometric data may be particularly invasive of privacy, and the risks of disclosure place additional importance on ensuring security of that data.[31] Accordingly, organizations should consider their arrangements with third parties in respect of confidentiality, security and separation of property; contingency planning; location of records; access and audit rights; subcontracting; and monitoring the material outsourcing arrangements.

In addition, OSFI has suggested that financial institutions consider employing "three lines of defense" approach articulated by the Basel Committee on Banking Supervision when assessing and implementing outsourcing arrangements.[32] The three lines of defense are the recommended practice for operational risk management, and include business line management; an independent corporate operational risk management function; and an independent review.

Conclusion

Ultimately, the success of any biometric identification system will require a high degree of user acceptance. The inherently personal nature of such information may raise concerns for customers of financial institutions about the collection, use, and storage of biometric data. Appropriate levels of transparency about the biometric system being deployed and the implementation of privacy safeguards are essential to providing customers with the assurance that their biometric information is being adequately protected.

At the same time, biometric technology continues to develop and expand the scope of the types of data that can be collected, used, and stored. As this rapid technological change continues, new and existing systems for biometric identification and authentication should be assessed and adjusted as necessary to account for the impact of those systems on customers' privacy interests and expectations.

The existing Canadian privacy law framework invokes a proportionality analysis when assessing new biometric identification systems. While existing privacy impact assessment methods can be successfully applied to new biometric identification technologies, the heightened privacy interests associated with biometric information warrants special attention. Further,

financial institutions may look to international standards for guidance on the implementation of biometric systems.

[*Editor's note*: **Molly Reynolds** practises civil litigation at Torys LLP, with a focus on corporate/commercial litigation and class actions, privacy and anti-spam, e-discovery, and administrative law.

Eliot Che practises civil litigation at Torys LLP, with a focus on corporate/commercial litigation, privacy, intellectual property and technology, administrative law and class actions.

Lara Guest is an articling student at Torys LLP who will be joining the Litigation and Dispute Resolution practice group as an associate.]

---

1 Apple, "iphone 6, Touch ID", <https://www.apple.com/iphone-6/touch-id/>; Samsung Galaxy S5, Features, <http://www.samsung.com/global/microsite/galaxys5/features.html>.

2 Windows, "Making Windows 10 More Personal and More Secure with Windows Hello" (March 17, 2015), <http://blogs.windows.com/bloggingwindows/2015/03/17/making-windows-10-more-personal-and-more-secure-with-windows-hello/>.

3 Privacy Commissioner of Canada, "Data at Your Fingertips" (2011) <https://www.priv.gc.ca/information/pub/gd_bio_201102_e.pdf>.

4 Tangerine, "Mobile Banking", <https://www.tangerine.ca/en/ways-to-bank/mobile-banking/index.html>.

5 TD Waterhouse Canada, "Voice Print System", <http://www.tdwaterhouse.ca/products-services/investing/td-direct-investing/trading-platforms/voice-print-system-index.jsp>.

6 CIBC, "Contactless and Mobile Payments", <https://www.cibc.com/ca/credit-cards/making-purchases/contactless-mobile-payments.html>.

7 Peter Belton, "In your irises: The new rise of biometric banking" *BBC News* (March 20, 2015), <http://www.bbc.com/news/business-31968642>.

8 Melissa Leong "Banking on biometrics: How you'll soon be able to pay with your finger, access an ATM with your eyes" *Financial Post* (December 6, 2014), online: <http://business.financialpost.com/personal-finance/banking-on-biometrics-how-youll-soon-be-able-to-pay-with-your-finger-access-an-atm-with-your-eyes>.

9 S.C. 2000, c. 5.

10 *Supra* note 8.

11 Office of the Privacy Commissioner of Canada, "Privacy Research Topic Index", <https://www.priv.gc.ca/information/research-recherche/sub_index_e.asp>.

12 *Ibid*.

13 R.S.C. 1985, c. P-21.

14 *Supra* note 3.

15 Office of the Privacy Commissioner of Canada, "Identity, Privacy and the Needs of Others to Know Who You Are: A Discussion Paper on Identity Issues" (2008), <https://www.priv.gc.ca/information/research-recherche/2008/ID_Paper_e.asp>.

16 [1986] S.C.J. No. 7, [1986] 1 S.C.R. 103.

17 [2011] C.P.C.S.F. No. 12.

18 *Supra* note 16.

19 Ann Cavoukian and Alex Stoianov, "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy" (March 2007) at pp. 5–7, Information and Privacy Commissioner of Ontario <https://www.ipc.on.ca/images/resources/bio-encryp.pdf>.

20 *Ibid*.

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

22 *Supra* note 3.

23 *Ibid*.

24 Office of the Privacy Commissioner of Canada, "Automated Facial Recognition in the Public and Private Sectors" (March 2013), <https://www.priv.gc.ca/information/research-recherche/2013/fr_201303_e.asp>.

25 *Ibid*.

26 Peter Belton, "In your irises: The new rise of biometric banking" *BBC News* (March 20, 2015), <http://www.bbc.com/news/business-31968642>.

27 FIDO Alliance, "About the FIDO Alliance", <https://fidoalliance.org/about>.

28 FIDO Alliance, "The FIDO Alliance Announces First FIDO Authentication Deployment − PayPal and Samsung Enable Consumer Payments with Fingerprint Authentication on New Samsung Galaxy S5", <https://fidoalliance.org/the-fido-alliance-announces-first-fido-authentication-deployment-%E2%88%92-paypal-and-samsung-enable-consumer-payments-with-fingerprint-authentication-on-new-samsung-galaxy-s5/>.

29 ISO/IEC JTC 1/SC 37, "Biometrics". Biometrics is a standardization subcommittee in the Joint Technical Committee ISO/IEC JTC 1 of the ISO and the International Electrotechnical Commission ("IEC"). These

groups develop and facilitate standards within the field of biometrics.

[30] The 28 participating members of ISO/IEC JTC 1/SC 37 are: Australia, China, Czech Republic, Denmark, Egypt, Finland, France, Germany, India, Israel, Italy, Japan, Republic of Korea, Malaysia, New Zealand, Norway, Poland, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Thailand, Ukraine, United Kingdom, and United States of America. The 13 observing members of ISO/IEC JTC 1/SC 37 are: Austria, Belgium, Bosnia and Herzegovina, Canada, Ghana, Hungary, Indonesia, Islamic Republic of Iran, Ireland, Kenya, Netherlands, Romania, and Serbia.

[31] Office of the Superintendent of Financial Institutions, "New technology-based outsourcing arrangements" (February 29, 2012), online: Government of Canada <http://www.osfi-bsif.gc.ca/eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/cldcmp.aspx>.

[32] *Ibid*.

National Banking Law Review is published six times per year by LexisNexis Canada Inc.
This issue is cited as 34 Nat. B.L. Rev.

You can contact the LexisNexis Editor at:

Telephone (905) 479-2665, ext. 308 Toll-Free Telephone 1-800-668-6481
Fax (905) 479-2826 Toll-Free Fax: 1-800-461-3275
Internet e-mail: nblr@lexisnexis.ca

Price: $465 for six issues and annual index. Binder available at $20 upon request.
$535 for Print & PDF

ISBN 0-409-91076-7 ISSN 0822-1081
ISBN 0-433-44389-8 (Print & PDF)
ISBN 0-433-44684-6 (PDF)

The Journal is indexed in the *Index of Canadian Periodical Literature*
and in *the Index to Canadian Legal Literature*.
Publications Mail Registration No. 180858