大成 DENTONS

At issue is the use of personal data through analytics to develop business intelligence. Two legal risks emerge: violation of privacy through inconsistency of use and lack of consent, which engages the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and discrimination through algorithmic bias, which engages the *Canadian Human Rights Act* (CHRA).

I Privacy risks

Financial institutions under federal jurisdiction are subject to PIPEDA, which sets the boundaries for data analytics through the following relevant provisions:

- section 3 limits the purposes for processing of personal information to those which “a reasonable person would consider appropriate in the circumstances”;
- section 7.1 prohibits use without consent except in cases of necessity, where consent is impracticable;
- clauses 4.3 and 4.5 of Schedule 1 prohibit use for purposes other than those for which the information was consented;
- section 6.1 defines valid consent to be achieved where it is reasonable to expect that the individual would understand the consequences of consenting;
- clause 4.3.6 of Schedule 1 clarifies that where the information is sensitive, generally express, rather than implicit, consent should be sought.

The most recent interpretation of these provisions is found in the Office of the Privacy of Canada Report of Findings into the Bell Canada Relevant Ads Program, #2015-01. The complaint alleged that serving relevant ads to Bell customers on the basis of analytics of the customers’ profiles based on their use of Bell services such as phone, internet or cable, except with opt-out, was a violation of PIPEDA. Of relevance here:

- the OPC determined that sending targeted, relevant ads was a new purpose, therefore subject to new consent ;
- the profile constituted sensitive personal information and therefore required express consent, therefore opt-in.

Against this backdrop, current applications of data analytics in financial services raise low to high compliance risk, all subject to case-by-case variables:

1. Low risk: the following applications may be deemed to be inherent to the purposes of financial service that the customer has consented to:

- fraud detection, through analysis of irregularities in transactions or spending patterns;
- improvement of customer interface with client feedback;
- specific risk assessment of reliability upon application for a loan or mortgage;
- assessment of loan reimbursement patterns for provision calculation to secure bank capitalisation and for early warning of default and debt collection.

Data analytics in these cases might be applied without new consent provided privacy policies are clear and prominent in describing these applications.

2. Medium risk: the following applications could be argued to constitute new purposes but close to what ‘a reasonable person would expect”:

- customer data management, for example to provide enhanced individual reports;
- identification of digital banking use, for example to improve customer experience or to offer relevant digital solutions;
- transaction channel identification to offer relevant services;
- loyalty creation such as offering rewards per transaction since the transactions already have to be monitored for fraud detection.

These applications of data analytics could be compliant with implied consent, therefore with an opt-out.

3. High risk: on the basis of the OPC’s Report of findings in Bell Canada, the following applications would appear to require express consent. They constitute a departure from the original purpose for which the information was provided and create sensitive personal information:

- auxiliary products cross-selling, beyond financial advice, on the basis of customer profiles or segmentation such as between “easy spenders “ or “cautious investors”;
- spending stimulation, for example such as targeting cautious investors to offer loans and encourage more active spending;
- sharing business intelligence with third parties to identify more products in accordance with client’s needs.

These applications would most likely be considered to be subject to express consent therefore require active opt-in.

II Algorithmic bias

For all the talk of “artificial intelligence”, humans are still behind machine learning and algorithm development. Hence, the introduction of bias in algorithms. For example, a Carnegie Mellon study found that Google ads for high-income jobs were served much more frequently to men than to women. Another organization found its algorithm was systematically excluding highly qualified African-American candidates because it erroneously took into account over-representation in the criminal justice system.

Companies seek to avoid algorithmic bias through the contribution of psychologists, semioticians, ethnographers, anthropologists and ethicists.

The legal boundaries on algorithmic bias are set through the CHRA, at section 3, specifying prohibited grounds of differentiation and section 5 defining “discrimination”. Together, they would prohibit data analytics that would differentiate access to financial institutions’ services or products adversely on the basis of “race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics, disability, and conviction of a criminal offence subject to a pardon or suspension.” (Section 3(1)).

It follows that these data elements should not be introduced in the creation of algorithms for business intelligence. Moreover, and this is the role of the experts mentioned above, the impact of algorithms should be assessed to avoid systemic, albeit unintentional, adverse differentiation corresponding to prohibited grounds.

Chantal Bernier, Counsel
National Practice Group Leader
Privacy and Cybersecurity
Dentons LLP Canada
+1 613 783-9684
chantal.bernier@dentons.com