PRIVACY IMPLICATIONS OF A REGISTRY OF BENEFICIAL OWNERSHIP UNDER THE CANADIAN LEGAL FRAMEWORK

大成 DENTONS

Setting the stage

1. Applicable laws

- *Canadian Charter of Rights and Freedoms*:
  - 8. Everyone has the right to be secure against unreasonable search or seizure.
  - 1. The *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society
- Privacy legislation:
  - Federal: *Privacy Act*, for the public sector; *Personal Information Protection and Electronic Documents Act* (PIPEDA) for the private sector
  - Alberta: *Freedom of Information and Protection of Privacy Act,* for the public sector; *Personal Information Protection Act*
  - British Columbia: *Freedom of Information and Protection of Privacy Act* for the public sector; *Personal Information Protection Act*
  - Manitoba: *Freedom of Information and Protection of Privacy Act*
  - New Brunswick: *Personal Health Information Privacy and Access Act*
  - Newfoundland and Labrador: *Access to Information and Protection of Privacy Act*
  - Northwest Territories: *Access to Information and Protection of Privacy*
  - Nova Scotia: *Freedom of Information and Protection of Privacy Act*
  - Nunavut: *Access to Information and Protection of Privacy*
  - Ontario: *Freedom of Information and Protection of Privacy Act*
  - Prince Edward Island: *Freedom of Information and Protection of Privacy Act*
  - Québec: *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* for the public sector; *Loi sur la protection des renseignements personnels dans le secteur privé*
  - Saskatchewan: *Freedom of Information and Protection of Privacy Act*

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, (PCMLTFA) section 72(2): bi-annual review by the Office of the Privacy Commissioner of Canada

2. A 4 Parts Privacy Compliance test

I. Legitimacy	II Security
III. Accountability	IV. Oversight

PART I – ESTABLISHING THE LEGITIMACY OF A REGISTRY – the Oakes Test (*R v. Oakes* [1986] 1 S.C.R. 103)

4 legitimacy criteria:

1. Necessity
2. Proportionality
3. Effectiveness
4. Least intrusive alternative

1. Necessity

"Canada currently ranks 70th in terms of ability to access information on companies, this is below Sri Lanka, El Salvador and Bahrain"

(http://compass.arachnys.com/rankings.html)

According to Transparency International Canada Beneficial Ownership Transparency, a registry is necessary for:

- Timely access to beneficial ownership information by competent authorities in Canada is restricted with no guarantee of timeliness
- information collected in the majority of provinces is insufficient to support the identification of the beneficial owner
- there is no guarantee that the information recorded in the province registries is accurate
- the PCMLTFA does not grant FINTRAC authority to examine or require production of any records that financial institutions and DNFBPs retain, including beneficial ownership information
- creating a public registry of the beneficial ownership of companies would :
- provide Canadian law authorities, journalists, civil society organizations and others with important corporate information.
- benefit tax authorities and law enforcement agencies in saving time and being able to investigate the ownership structure of a company without tipping off the company that they are under investigation.
- making this information publicly available has advantages in terms of public scrutiny, building public trust and ensuring investors, the market and other companies know better with whom they are doing business.

2. Proportionality

Europe has addressed proportionality to that necessity with respect to privacy:

- registers only be accessible to 'competent authorities', financial intelligence units, obliged entities and "persons who can demonstrate a legitimate interest to access the information", and not the wider public.
- Information accessible to the wider public is filtered to what is necessary in relation to beneficial owners as "economic actors"

Under 2016 Proposal to amend 4AMLD:

- "given that it is necessary to balance the legitimate request for anonymity of payments by individuals with the requirements of effectively monitoring suspicious transactions, and given latest market trends and figures that indicate the average amounts of non-suspicious transactions with anonymous prepaid instruments, it is appropriate and proportionate to reduce the thresholds set out in the 4AMLD for transactions for which customer due diligence is not performed;
- "a distinction made between categories of legal entities engaged in the management of trusts as a business, with a view to gain profit, and other categories. It is legitimate and proportionate to grant public access to a limited set of information on the beneficial owners of the first category of legal entities, while, in respect of the second category, such beneficial ownership information should only be made known to persons and organisations demonstrating a legitimate interest."
- "Member States to disclose via a register beneficial information for companies and business-type trusts and other similar legal arrangements, while retaining the necessity to demonstrate a legitimate interest for access to that information in respect of trusts and other legal arrangements that do not qualify as business-type."
- "Extending the scope of the 4AMLD to virtual currency exchange platforms was duly analysed from the perspective of the rights to private life and the protection of personal data. AML/CFT legislation requires obliged entities to know their customers – as well as certain other persons who are not always their customers (e.g. beneficial owners) – and to assess their associated money laundering and terrorist financing (ML/TF) risks. For that purpose, obliged entities need to collect, process and record personal data, and sometimes to share such data with public authorities (such as FIUs) or with private entities within the same group. These requirements have implications for private persons while having an overall security impact (general interest). The proposed amendments are formulated in a clear and proportionate manner, setting out the required safeguards, and the Commission considers this necessary in order to achieve the objectives of enhancing the effectiveness of the fight against ML/FT and complying with new international standards. In addition, positive effects for consumers are expected as a result of the proposed rules on designating virtual currency exchange platforms as obliged entities. Reducing anonymity surrounding virtual currencies will contribute to increasing trust of their good-faith users"
- "From a data protection perspective, new obliged entities are designated, and they will have to process personal data (i.e. by performing customer due diligence). This new obligation established for public policy considerations is counter-balanced by the insertion of clear definitions of the obliged entities, who are informed of the new obligations they become subject to (collection and processing of financial personal data online) and the data protection elements that are specific to these obligations."
- Article 18 of the Directive requires obliged entities to apply enhanced customer due diligence (ECDD measures) when dealing with natural or legal entities established in high risk third countries. Article 9 of the 4AMLD empowers the Commission to identify – by way of a delegated act - high-risk third countries that have deficient AML/CFT regimes in place, and therefore constitute an important risk for terrorist financing. That delegated act is to be adopted – and submitted to the scrutiny of the European Parliament and the Council – in July 2016.
- Disclosure of BOI will be limited to:
  - Name
  - month and year of birth
  - nationality
  - country of residence
  - nature and extent of the beneficial interest held

3. Effectiveness

In the EU:

- Central registers make it easier for regulators and prosecutors to identify potential wrongdoing and to identify those businesses who are either intentionally or unknowingly caught up in illicit activity.
- Financial services firms will have access to a wider range of information in order to conduct customer due diligence.
- Significant gaps in the transparency of financial transactions around the world have been revealed which indicate that offshore jurisdictions are often used as locations of intermediary entities that distance the real owner from the assets owned, often to avoid or evade tax."
- Preventing "large-scale concealment of funds which can hinder the effective fight against financial crime, and to ensure enhanced corporate transparency so that true beneficial owners of companies or other legal arrangements cannot hide behind undisclosed identities."

4. Least intrusive alternatives

In the UK:

The register will hold the following information on the beneficial owners:

- full name and date of birth;
- nationality;
- country or state of residence; and
- residential address and service address.
- date on which beneficial interest in the company was acquired and the nature of the beneficial interest itself.

BUT,

- The register will withhold the full dates of birth and residential addresses of the beneficial owners from the publicly accessible data.
- There will be only two locations from which the register can be accessed; directly via the company or through the central register (as a result of the annual filing requirement).
- Access is limited to "a proper purpose"

In the EU:

- Competent authorities granted access to the central register shall be those public authorities with designated responsibilities for combating money laundering or terrorist financing, including, tax authorities and authorities that have the function of investigating or prosecuting money laundering, associated predicate offences and terrorist financing and seizing or freezing and confiscating criminal assets.";

- in order to respect privacy and protect personal data,
  - such registries should store the minimum data necessary to the performance of AML/CFT investigations,
  - the concerned data subjects should be informed that their data are recorded and accessible by FIUs and are given a contact point for exercising their rights of access and rectification.
  - maximum retention periods (supported by adequate reasoning as to their duration) should be applicable to the registration of personal data in registries
  - provision should be made for their destruction once the information is no longer needed for the stated purpose
  - access to such registries and databases should be limited on a "need to know" basis.

From the proposal to amend 4AMLD:

(26) A fair balance should be sought in particular between the general public interest in corporate transparency and in the prevention of money laundering and the data subjects' fundamental rights. The set of data to be made available to the public should be limited, clearly and exhaustively defined, and should be of a general nature, so as to minimize the potential prejudice to the beneficial owners. At the same time, information made accessible to the public should not significantly differ from the data currently collected. In order to limit the interference with the right to respect for their private life in general and to protection of their personal data in particular, that that information should relate essentially to the status of beneficial owners of businesses and trusts, and should strictly concern the sphere of economic activity in which the beneficial owners operate.

(27) The disclosure of beneficial ownership information should be designed to give governments and regulators the opportunity to respond quickly to alternative investment techniques, such as cash-settled equity derivatives. On the other hand, legitimate majority shareholding should not be deterred from taking an active role in monitoring management in listed companies. For the functioning of financial markets that have become increasingly internationally-oriented and complex, it is essential that legal rules and requirements that enable information sharing on an international level be available and effectively implemented by national supervisory authorities.

(28) The personal data of beneficial owners should be publicly disclosed in order to enable third parties and civil society at large to know who the beneficial owners are. The enhanced public scrutiny will contribute preventing the misuse of legal entities and legal arrangements, including tax avoidance. Therefore, it is essential that this information remains publicly available through the national registers and through the system of interconnection of registers for 10 years after the company has been struck off from the register. However, Member States should be able to provide by law for the processing of the information on beneficial ownership, including personal data for other purposes if such processing meets an objective of public interest and constitutes a necessary and proportionate measure in a democratic society to the legitimate aim pursued.

(29) Moreover, with the same aim of ensuring a proportionate and balanced approach and to guarantee the rights to private life and personal data protection, Member States should provide for exemptions to the disclosure of and to the access to beneficial ownership information in the registers, in exceptional circumstances, where the information would expose the beneficial owner to the risk of fraud, kidnapping, blackmail, violence or intimidation.

PART II: ENSURING DATA SECURITY

In the EU: EU data protection directives and *General Data Protection Regulation* coming on May 25 2018 applies to the processing of personal data under this AML Directive.

In Canada, under the *Privacy Act*:

- 4 No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution
- 5 (1) A government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates (…)

  (2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.
- 6 (1) Personal information that has been used by a government institution for an administrative purpose shall be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information.

  (2) A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible.
- 8 (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section:
  - (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

For Canada under PIPEDA:

- 7(3) (…)an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is
- (…)
- c.2) made to the government institution mentioned in section 7 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act as required by that section (reporting to FINTRAC)

Part III: ENSURING ACCOUNTABILITY

Under the *Privacy Act*, Treasury Board Secretariat Directive on Privacy Impact Assessments (PIAs):

5.1 Objectives

5.1.1 To provide direction to government institutions with respect to the administration of PIAs for new or substantially modified programs and activities involving the creation, collection and handling of personal information; and

5.1.2 To ensure, through the conduct of PIAs, sound management and decision making as well as careful consideration of privacy risks with respect to the creation, collection and handling of personal information as part of government programs or activities

5.2 Expected results

5.2.1 PIAs are conducted in a manner that is commensurate with the level of privacy risk identified prior to establishing any new or substantially modified program or activity involving personal information.

5.2.2 Privacy practices that comply with legal and policy requirements related to the administration of the Privacy Act are implemented.

5.2.3 The public reporting of personal information under the control of government institutions is complete, accurate and up to date.

PART IV: OVERSIGHT

- As an Officer of Parliament charged with the oversight of the Privacy Act, the Privacy Commissioner has broad powers of investigation and review and can request additional project documentation related to the planning, assessment or implementation of new or substantially modified programs or activities that involve personal information or have an impact on the privacy of Canadians and of those individuals present in Canada. (TBS PIA Directive)
- Courts

Outstanding privacy issues – The least intrusive measure to ensure effectiveness of the registry:

- What beneficial owners should register?
- What is their reasonable expectation of privacy?
- What information is truly necessary?
- Who should have access to the registry?
- What constitutes "proper purpose" (UK) or "legitimate interest" (EU) to access the registry?
- How long should the information be kept?
- What data security mechanisms would be required?
- What compliance mechanisms would be commensurate would be commensurate?
- What oversight mechanisms would ensure both effectiveness and privacy?

Chantal Bernier
Counsel
Dentons LLP Canada
Global Privacy and Cybersecurity Group
Government Affairs and Public Policy Group
+1 613 783-9684
chantal.bernier@dentons.com