THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Improving Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

CANADIAN BAR ASSOCIATION
BUSINESS LAW, CHARITIES AND NOT-FOR-PROFIT LAW, CRIMINAL JUSTICE, INTERNATIONAL LAW, PRIVACY AND ACCESS SECTIONS, ETHICS AND PROFESSIONAL RESPONSIBILITY SUBCOMMITTEE, AND ANTI-CORRUPTION TEAM

AUGUST 2023

66 Slater St., Suite 1200, Ottawa, ON, Canada K1P 5H1
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

PREFACE

The Canadian Bar Association is a national association representing 37,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the Canadian Bar Association's Business Law, Charities and Not-For-Profit Law, Criminal Justice, International Law, Privacy and Access Sections, Ethics and Professional Responsibility Subcommittee and the Anti-Corruption Team, with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the Canadian Bar Association's Business Law, Charities and Not-For-Profit Law, Criminal Justice, International Law, Privacy and Access Sections, Ethics and Professional Responsibility Subcommittee and the Anti-Corruption Team.

TABLE OF CONTENTS

Improving Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

I. INTRODUCTION 1

II. CBA COMMENTS 1

A. CHAPTER 3 (Federal, Provincial, and Territorial Collaboration) 2

1. How can different orders of government better collaborate and prioritize AML/ATF issues related to beneficial ownership? 2
2. What is the legal profession's role regarding AML/ATF? 3

B. CHAPTER 4 (Criminal Justice Measures to Combat Money Laundering and Terrorist Financing) 6

1. Should the government consider sentencing reforms for the offence of laundering proceeds of crime? 6
2. Should the *Criminal Code* be amended to include an order for subscriber information? 6
3. Should the *Criminal Code* be amended to provide explicitly for the inclusion of a power to search a person for a thing or property set out in a warrant under section 487 or under section 462.32 where the peace officer has reasonable grounds to believe that the person has the thing on their person? 11
4. Are there are other measures that could facilitate preservation of proceeds of crime under the *Criminal Code*? 13

C. CHAPTER 5 (Canada Financial Crimes Agency) 13

1. What are the considerations for a Canada Financial Crimes Agency (CFCA)? 13

D. CHAPTER 6 (Information Sharing) 14

1. What types of information would be most valuable to share amongst reporting entities to detect, disrupt, and facilitate prosecution of money laundering and terrorist financing offences? 14
2. Are there specific tools, mechanisms, or models from other jurisdictions that could be incorporated into Canadian legislation to support greater information sharing? 14
3. What guardrails would best protect personal information while allowing for additional information to be exchanged between organizations? 15

4. How can the government enhance two-way information sharing between FINTRAC and the private sector? 15

5. Are there additional guidance or strategic intelligence products FINTRAC should look to provide to reporting entities and the public? 15

6. Should the government create and maintain a database of politically exposed persons (PEPs), heads of international organizations (HIOs), and their family members and close associates? 15

7. How could the government improve outreach and engagement with the non-profit sector on AML/ATF matters? 16

E. CHAPTER 9 (National and Economic Security) 16

1. Should FINTRAC take a more proactive role in combatting sanctions evasion? 16

III. CONCLUSION 17

Improving Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

I. INTRODUCTION

We are writing on behalf of the Canadian Bar Association's Business Law, Charities and Not-For-Profit Law, Criminal Justice, International Law, Privacy and Access Sections, Ethics and Professional Responsibility Subcommittee, and Anti-Corruption Team (CBA Sections) to respond to the Government of Canada consultation on how to improve Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime.

The CBA is a national association of over 37,000 lawyers, law students, notaries, and academics, and our mandate includes seeking improvements in the law and the administration of justice.

The Business Law Section's mandate covers the law governing corporate entities and includes securities regulation, commercial law and consumer law. The Charities and Not-For-Profit Law Section includes lawyers who advise or serve on the boards of charitable and other not-for-profit organizations – or are otherwise involved with the law and practice related to the charitable and not-for-profit sector. Criminal Justice Section members include prosecutors, defense counsel and legal academics specializing in criminal law. The International Law Section addresses issues of public and private international law including treaties and conventions, international trade, anti-corruption, international development and human rights. The CBA Privacy and Access Law Section's mandate is to review and influence privacy and access to information law and policy. The Ethics and Professional Responsibility Subcommittee fosters and advances ethical and professional conduct and standards in the legal profession. The Anti-Corruption Team advocates on behalf of the legal profession to end corrupt practices.

II. CBA COMMENTS

We offer the following comments in response to specific questions identified in the consultation paper.

A. CHAPTER 3 (Federal, Provincial and Territorial Collaboration)

1. How can different orders of government better collaborate and prioritize AML/ATF issues related to beneficial ownership?

The CBA fully supports efforts to combat financial crime and ensure corporate vehicles are not used for nefarious purposes. We recognize that money laundering and terrorist financing pose serious threats to the integrity of the Canadian economy and the security of its residents.

However, the approach to public access to beneficial ownership information must take into account legitimate and sensitive reasons for individuals wishing to maintain their privacy and confidentiality. The overarching purpose of a beneficial ownership registry is that the data it contains is accurate and allows law enforcement and other relevant authorities to better detect when corporate vehicles are used for financial crimes. Canada's federal beneficial ownership registry should appropriately balance individual rights and the public interest.

The CBA recently commented on beneficial ownership transparency in the context of Bill C-42, *An Act to amend the Canada Business Corporations Act*. CBA submission on Beneficial Ownership Transparency (June 2023).

The CBA submission referred to a 2022 decision of the Court of Justice of the European Union (CJEU) examining an anti-money-laundering directive (a 2019 Luxembourg law) establishing a Register of Beneficial Ownership where some information on the beneficial owners was accessible to the general public. The CJEU held that the directive was invalid because the public's access to information on beneficial ownership constituted a serious interference with the fundamental rights to respect for private life and to the protection of personal data. The CJEU held that the interference was neither limited to what is strictly necessary nor proportionate to the objective pursued.

In response, the European Parliament announced a revised directive on the use of the financial system for the purposes of money laundering or terrorist financing. The new directive establishes that persons with a "legitimate interest," such as journalists, researchers and civil society organizations, should be able to access the registry. Once established, their access right will be valid for at least two and a half years.

By way of update, as of June 13, 2023, a new EU regulation confirms that the public will no longer have access to national transparency registries and instead individuals must prove that they have a "legitimate interest" in the information before it can be obtained.

In our view, the general public should not be granted unfettered access to personal and sensitive information in the beneficial ownership registry. Individuals should demonstrate a "legitimate interest" to access the registry. This could include journalists, researchers and civil society organizations, upon application. The access should be time-limited (valid for a reasonable amount of time) and scope-limited (where a person could request access about a group or family of companies but not granted bulk access).

2. What is the legal profession's role regarding AML/ATF?

The consultation paper recognizes the Supreme Court of Canada's 2015 decision stating that the requirements of the AML/ATF framework, as applied to the legal profession, violated the *Charter.*[1] It adds that the exclusion of the legal profession in Canada's AML/ATF framework was considered a major deficiency in the Financial Action Task Force's (FATF) 2016 evaluation of Canada.

To say there is an absence of AML/ATF obligations on lawyers is inaccurate.

Comprehensive anti-money laundering and anti-terrorist financing regulations are imposed on legal professionals by Canada's law societies, coordinated through the Federation of Law Societies of Canada (Federation). A consistent and robust framework to address the risks that can arise in the provision of legal services is of critical importance and should not be ignored.

Law societies regulate the legal profession in the public interest. The AML/ATF rules and regulations implemented by provincial and territorial law societies (based on Model Rules created by the Federation) address the conduct of legal professionals to prevent them from unwitting involvement in money laundering or financing terrorism.

In addition, legal professionals must abide by extensive professional conduct requirements including rules that prohibit them from knowingly assisting in or encouraging any unlawful conduct. Law societies have extensive investigatory powers including the power to compel production of documents or other records and to answer questions posed by the regulators. Legal professionals are also subject to criminal laws and anyone who willingly or recklessly participates in criminal activity is subject to prosecution.

---

1 *Canada (Attorney General) v. Federation of Law Societies of Canada,* 2015 SCC 7, [2015] 1 SCR 401

Constitutional Principles

This consultation offers an opportunity to revisit the 2015 Supreme Court of Canada decision in *Canada (Attorney General) v. Federation of Law Societies of Canada.*[2] In that case, the Court held that the parts of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) obliging legal counsel to collect information not required for client representation and granting expansive powers to search law offices violated the *Charter* and undermined the ability of legal professionals to comply with their duty of commitment to their client.

The Court held that the principles governing searches of law offices in *Lavallee, Rackel & Heintz v. Canada (Attorney General)*[3] apply and found that the legislation did not comply with those standards, resulting in an infringement of the section 8 *Charter* right to be free of unreasonable searches and seizures.

Justice Cromwell stated:

> [44] The core principle of the decision is that solicitor-client privilege 'must remain as close to absolute as possible if it is to retain relevance': Lavallee, at para. 36. This means that there must be a 'stringent' norm to ensure its protection, such that any legislative provisions that interfere with the privilege more than 'absolutely necessary' will be found to be unreasonable.

The Court also considered whether another central component of the solicitor-client relationship – the lawyer's duty of commitment to the client – required constitutional protection against government intrusion. The Court held that it did, for many of the same reasons that support constitutional protection for solicitor-client privilege.

Justice Cromwell stated:

> [83] […] A client must be able to place 'unrestricted and unbounded confidence' in his or her lawyer; that confidence which is at the core of the solicitor-client relationship is a part of the legal system itself, not merely ancillary to it: […] The lawyer's duty of commitment to the client's cause, along with the protection of the client's confidences, is central to the lawyer's role in the administration of justice.

---

2 *Ibid*

3 *Lavallee, Rackel & Heintz v. Canada (Attorney General)*, 2002 SCC 61, [2002] 3 S.C.R.209

Justice Cromwell further discussed the duty of commitment to the client:

> [96] Clients – and the broader public – must justifiably feel confident that lawyers are committed to serving their clients' legitimate interests free of other obligations that might interfere with that duty. Otherwise, the lawyer's ability to do so may be compromised and the trust and confidence necessary for the solicitor-client relationship may be undermined. The duty of commitment to the client's cause is an enduring principle that is essential to the integrity of the administration of justice. In *Neil*, the Court underlined the fundamental importance of the duty of loyalty to the administration of justice. The duty of commitment to the client's cause is an essential component of that broader fiduciary obligation.

Enhancing Effectiveness

The consultation paper explores ways to enhance the effectiveness of the AML/ATF regime to investigate and prosecute money laundering and terrorist financing and deprive criminals of the proceeds of crime. Chapter 2 references the Report on Performance Framework for Canada's AML/ATF Regime which noted that results for investigations, prosecutions and forfeitures declined over the past decade.

It is useful to contrast those findings with legal professionals and the extensive AML/ATF and professional conduct rules with which they must comply (and the ability of law societies to enforce those rules).

As Canadian and international concerns over money laundering and terrorism financing have grown, Canadian law societies have tightened rules on client identification, verification and the receipt of cash by lawyers. These new rules for lawyers are in line with rules applicable to other businesses that handle funds and are subject to FINTRAC.

Since implementing the Model Rules, law societies have prepared educational resources and practice advice materials to assist lawyers. An AML/ATF Working Group prepared, among other resources, 1) a comprehensive guide to the rules and professional responsibility, 2) risk advisories addressing client and transaction risks that arise in certain areas of practices, and 3) a collection of risk assessment case studies.

Different tools are used by law societies to ensure compliance with regulatory obligations such as self-reporting, practice reviews and audits (random and risk-based). Law societies have extensive investigatory and audit powers. Investigations can result in disciplinary action, including disbarment.

Any assessment of Canada's AML/ATF regime should acknowledge that the comprehensive AML/ATF rules and professional conduct requirements for legal professionals complement the government's framework and address concerns about the "inherent risks" in the delivery of legal services.

Collaborative Approach

The consultation paper notes that since June 2019, the government has worked closely with the Federation to explore money laundering and terrorist financing in the legal profession and strengthen information sharing between law societies and the Government of Canada. Specific objectives include sharing information on data, trends and money laundering typologies, compliance and enforcement. The CBA supports this collaborative approach.

B. CHAPTER 4 (Criminal Justice Measures to Combat Money Laundering and Terrorist Financing)

1. Should the government consider sentencing reforms for the offence of laundering proceeds of crime?

Yes. Among other things, stronger penalties should be considered. Stronger penalties would offer 1) increased deterrence, 2) punishment of offenders as social policy enforcement, and 3) increased respect for Canada as a "rule of law" nation that enforces its own laws consistent with international legislative and policy best practices.

However, proper implementation would require sufficient political will and financial commitments, which have proven difficult to date.

2. Should the *Criminal Code* be amended to include an order for subscriber information?

It is unclear why the present consultation includes a section on warrantless access to customer information, as the consultation paper does not identify how this is connected to the investigation and enforcement of anti-money laundering and anti-terrorist financing laws.

Previous proposals for lawful access were first framed as necessary to combat child pornography, and later, after tragic deaths of young people, as essential to address cyberbullying.

Meaningful and well-informed public consultation on enhanced investigative capabilities for law enforcement should frame those capabilities simply for what they are – additional police

powers that may be needed to keep pace with technological advancements. This characterization allows the public to assess their potential value and impact on privacy and *Charter* rights, without reacting emotionally to egregious criminal or terrorist activities.

The Supreme Court's decision in *R. v. Spencer*[4] may have significantly exacerbated the problems for police – the protection of *Charter* rights generally has the effect of constraining police powers.

The CBA has consistently called for judicial pre-authorization for the seizure of subscriber information.

Former Bill C-30, *Protecting Children from Internet Predators Act* proposed an administrative regime where "designated" peace officers could obtain subscriber information without judicial authorization. The proposal in the consultation paper raises the same concerns: the scope of information that may be included in "subscriber information" needs to be carefully tailored and not extend beyond what might be appropriately regarded as 'basic information.'

Bill C-30 contained no limit on how much customer information could be requested at once and could be used to demand the names and addresses of all customers with IP addresses in a particular range. An information demand could be made in the absence of a legitimate investigation with the subject never given notice that a request was made. Finally, there was no mechanism for a telecommunications service provider to challenge an overly broad request.[5]

Former Bill C-47, *Technical Assistance for Law Enforcement in the 21st Century Act* included a vast list of data points that would be considered "basic subscriber information": name, address, telephone number and electronic mail address of any subscriber to any of the service provider's telecommunications services and the Internet protocol address, mobile identification number, electronic serial number, local service provider identifier, international mobile equipment identity number, international mobile subscriber identity number and subscriber identity module card number that are associated with the subscriber's service and equipment.

---

4 2014 SCC 43.

5 This was seen as essential by the court in *R. v Rogers Communications*, 2016 ONSC 70. The court further suggested that a telecommunications service provider may have an obligation to assert the privacy interests of its clients.

While these proposed powers never came to be, the proposals for "lawful access" to customer information had no limitation on how they would be used, what types of investigations were permissible and how broadly the net could be cast. Under these proposals, police could have demanded names, addresses and IP addresses of every customer. Police would have been able to obtain the names, addresses, email addresses and phone numbers of every person who attended a lawful gathering. This could have been done without any oversight or accountability.

The Supreme Court of Canada in *R. v. Spencer*[6] was clear that Canadians have a right to anonymity as a dimension of informational privacy:

> [T]he police request to link a given IP address to subscriber information was in effect a request to link a specific person (or a limited number of persons in the case of shared Internet services) to specific online activities. This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized by the Court in other circumstances as engaging significant privacy interests… I conclude therefore that the police request to Shaw for subscriber information corresponding to specifically observed, anonymous Internet activity engages a high level of informational privacy.

To be constitutional, any demand for subscriber information must be authorized by a judge, made in exigent circumstances or be based on a reasonable law. The *Spencer* decision impels a legislative response to govern the lawful seizure of subscriber information.

The consultation paper suggests that judicial authorization may be too onerous for the early stages of investigation, and that law enforcement are presently unable to obtain information on a standard of 'suspicion.' In fact, various *Criminal Code* sections provide for judicial authorizations in the early stages of investigations on a threshold of 'reasonable suspicion.'

The current requirement for a general production order under s. 487.018 requires reasonable grounds to suspect that (a) an offence has been or will be committed, and (b) the document or data is in the person's possession or control and will afford evidence respecting the commission of the offence.

---

6 2014 SCC 43. This case discussed if was lawful for a police agency to ask a telecommunications company for subscriber information, and for the telecommunications agency to disclose it.

This is a low threshold. If the police do not have reasonable grounds to suspect that an offence has been or will be committed and the recipient of the order will afford evidence, they should not be able to obtain this information. The *Criminal Code* places the ultimate decision on an independent judicial officer, not a law enforcement officer who has a structural bias in favour of officers in their agency.

If the production order process is unduly laborious and time-consuming, increasing the number of judicial officers available to review applications is a better solution than removing important checks and balances.

When obtaining judicial authorization is impractical in situations of imminent harm or exigent circumstances, the templates are sections 184.1 and 184.4 of the *Criminal Code* which permit peace officers to intercept communications without judicial authorization in those circumstances. Section 184.4 was scrutinized by the Supreme Court of Canada in *R. v. Tse*, resulting in more stringent limitations.[7]

Bill C-30 would have permitted peace officers to obtain subscriber information without judicial authorization in defined exceptional circumstances. We suggest taking another look at that provision, rather than it being "thrown out with the bathwater."

Making judicial authorization the norm, with an administrative provision for exceptional circumstances, would be preferable to a wholesale administrative regime like those that have engendered inconsistency and controversy in other countries.

Concerns about the scope and nature of such information, and the mechanisms by which it would be acquired must be measured against Canada's constitutional principle of a reasonable expectation of privacy. This principle defines the threshold at which prior judicial authorization for a search will be required. It is sometimes difficult to determine precisely where that threshold will fall but the Supreme Court of Canada has noted that this is a contextual exercise, requiring a careful balance between the rights of the individual and the legitimate interests of society in effective law enforcement. This careful balancing, when rights are at stake, cannot be carried out by a law enforcement officer.

As technology and investigative practices evolve, activities previously deemed constitutional without a warrant, may now require a warrant. For example, the extent to which changes in

---

7 *R. v. Tse*, 2012 SCC 16, [2012] 1 SCR 531.

technology and practice now allow for the discovery of core biographical information or intimate lifestyle details mean prior judicial authorization is required. Further, the current technological capability to combine various sources of information to reveal additional details about individuals is significant and may favour prior judicial authorization. Since the *Spencer* decision, it is clear that all of these factors weigh in favour of prior judicial authorization.

With respect to law enforcement's allegations that the 30-day default turnaround for general production orders hampers their investigations, it must be noted that organizations that receive these orders generally turn them around more quickly than the 30-day default.

But if a request is overly broad, unreasonable or otherwise challengeable, the organization needs a reasonable amount of time to determine if it will seek to challenge or overturn the production order. As noted above, the Ontario Superior Court of Justice has determined, in the face of a grossly overreaching (and judicially authorized) production order, organizations not only have standing to assert their customers' privacy interests, but they may also have an obligation to do so.[8] Except in exigent circumstances, organizations should have an adequate opportunity to seek legal advice and evaluate their own and their customers' interests.

Administratively authorized search procedures (as opposed to court ordered procedures), are particularly susceptible to abuse. In the US, a review of National Security Letters issued under the *Patriot Act* revealed significant irregularities and abuse in the program.[9] The Office of the Inspector General documented that those letters increased exponentially after the *Patriot Act* expanded that power. Difficulties and discrepancies in internal record keeping complicated the compilation of accurate information and statistics about their use. This experience should be a warning for Canada about administrative programs, as it shows that significant problems can arise even with a program that includes internal restrictions and safeguards.

Our concern about warrantless access to subscriber information is heightened when the privacy interests engaged are not recognized by those seeking change in this area, despite the *Spencer* decision. Law enforcement is generally dismissive and cavalier about the privacy interests at stake, suggesting this is just the sort of information found in a phone book.[10] This

---

8 *R. v. Rogers Communications*, 2016 ONSC 70.

9 A Review of the Federal Bureau of Investigation's Use of National Security Letters, March 2007, United States Department of Justice, Office of the Inspector General, Executive Summary at 34-50. Available online.

10 See Canadian Broadcasting Corporation. *Opposition jumps on surveillance bill confusion*, 20

suggests that if an administrative process were established outside of the oversight of an independent judicial officer, that process may not be exercised sparingly.

If any changes are made to create a police power to obtain customer information without judicial authorization (which we do not recommend), the law should require police to notify the affected person promptly unless doing so would compromise an active investigation. Further, a copy of each authorization should be given to an appropriate civilian oversight agency for the law enforcement agency, with annual reporting on the number of authorizations issued, nature of the offences investigated and number of individuals implicated.

3. Should the *Criminal Code* be amended to provide explicitly for the inclusion of a power to search a person for a thing or property set out in a warrant under section 487 or under section 462.32 where the peace officer has reasonable grounds to believe that the person has the thing on their person?

The consultation paper notes that electronic devices such as mobile phones can present particular challenges in the investigation of serious offences. It describes how issues arise as the *Criminal Code* provisions were not developed for the digital age or modern investigative search requirements. Although mobile devices may contain a significant amount of information useful to law enforcement, the extent of information raises important legal considerations including privacy rights under s. 8 of the *Charter*. Modernizing search powers to take into account mobile computing devices calls for strengthening privacy protection, not relaxing it.

The consultation paper refers to solicitor-client privilege considerations in the context of the Supreme Court of Canada's 2002 *Lavallee* decision which held that s. 488.1 of the *Criminal Code* (which sets out a procedure for determining a claim of solicitor-client privilege in relation to documents seized form a law office under a warrant) constituted an unreasonable search and seizure under s. 8 of the *Charter*.

The consultation paper describes how the Supreme Court outlined ten principles to guide Parliament in legislating searches of law offices to adequately protect solicitor-client privilege and how courts have developed similar principles relating to investigatory techniques such as wiretaps where communications protected by solicitor-client privilege may be involved. The consultation paper indicates that some parties have expressed concerns that the current

---

February 2012, online. The Privacy Commissioner of Canada explores the nature of information and its privacy implications in *What an IP Address Can Reveal About You*, May 2013, online.

framework, using a referee to review and manage any material on electronic devices that is protected by solicitor-client privilege, is "unwieldy and time-consuming."

This consultation offers a further opportunity to reiterate the importance of respecting Canada's constitutional framework, including solicitor-client privilege.

When considering the effectiveness of the *Lavallee* principles, it is imperative to return to first principles and re-examine the findings of the Supreme Court of Canada. The Court held that where the interest at stake is solicitor-client privilege, the usual exercise of balancing privacy interests and the exigencies of law enforcement is not particularly helpful because the privilege favours not only the privacy interests of a potential accused, but also the interests of a fair, just and efficient law enforcement process.

Finding that solicitor-client privilege must remain as close to absolute as possible, the Court stated it must adopt stringent norms to ensure its protection. The Court determined that the procedure in s. 488.1 must minimally impair solicitor-client privilege to pass *Charter* scrutiny. The section more than minimally impaired the privilege, so it amounted to an unreasonable search and seizure.

The *Lavallee* principles have been applied in numerous cases and in different contexts. For example, the *Lavallee* rules on searching law offices will include "any place where privileged documents might reasonably be expected to be located."[11] Also, those conducting the search of a law office have a duty to minimize the impairment of solicitor-client privilege.[12]

In recent years, case law has developed in the area of searching electronic devices where the court has taken steps to balance the need to preserve solicitor-client privilege while providing for an efficient search.

For example, in *Solicitor-Client Privilege of Things Seized (Re*),[13] the unnamed party asserted privilege over electronic data and documents stored electronically and seized as part of an *Income Tax Act* investigation. The search was suspended pending the identification and

---

11 *Festing v. Canada (A.G.)* 2003 BCCA 112 (CanLII) at par. 24

12 *Maranda v. Richer* 2003 SCC 67 at paragraphs 14-20

13 *Solicitor -Client Privilege of Things Seized (Re,)* 2019 BCSC 91

isolation of solicitor-client privileged materials. The parties could not agree on an appropriate person and procedure to identify, isolate and store the solicitor-client privileged materials.

The court found that because the client's interests were different than the search of a lawyer's office, a referee need not be appointed. An "operationally-independent forensics department with technical expertise" may be permitted to isolate solicitor-client privilege materials. However, the tools used in the isolation process must allow the forensics team to do the work without reading the content of the privileged material. The court held that key words (used in searches) that disclose privileged information are not acceptable. The court also stated that the examiner should be able to take an oath of confidentiality. The court stipulated that the process of identifying, isolating and storing data that may be subject to a solicitor-client privilege claim must be reasonable, which requires that it comply with a standard of minimal impairment.

As stated by the Court in *Lavallee*, privilege is a positive feature of law enforcement, not an impediment to it. We are concerned that this positive feature is too often viewed as a principle that results in time-consuming or otherwise challenging processes in investigations, rather than as a foundational principle in our democratic society and fundamental to the rule of law.

4. Are there are other measures that could facilitate preservation of proceeds of crime under the *Criminal Code*?

A properly staffed and funded division of the RCMP dedicated to "economic crime" investigation and prosecution, including money laundering and terrorist financing, would help. The benefits would include improved enforcement and deterrence in the realm of economic criminal laws, including money laundering and terrorist financing. However, implementation would require sufficient political will and federal funding, which have proven difficult to date.

C. CHAPTER 5 (Canada Financial Crimes Agency)

1. What are the considerations for a Canada Financial Crimes Agency (CFCA)?

Creating a Canada Financial Crimes Agency (CFCA) must not result in unnecessary expense, redundancy and competition between agencies. The CFCA should have a clear mandate that works collaboratively with other agencies, including the RCMP.

D. CHAPTER 6 (Information Sharing)

1. What types of information would be most valuable to share amongst reporting entities to detect, disrupt, and facilitate prosecution of money laundering and terrorist financing offences?

The following types of information are generally considered useful in achieving these aims:

a) Transaction data: Information about financial transactions, such as amounts, parties involved, and transaction dates;

b) Customer information: Data related to customers or clients involved in transactions, including their identification documents, addresses, and business affiliations;

c) Suspicious activity reports: Details on any suspicious transactions or activities that could indicate potential money laundering or terrorist financing;

d) Beneficial ownership information: Data on the ultimate beneficial owners of corporations or assets involved in transactions to understand the actual control and ownership;

e) Risk assessments: Information on the risk levels associated with certain clients, transactions, or jurisdictions to prioritize monitoring efforts;

f) Politically exposed persons (PEPs) data: Knowledge of individuals who hold prominent public positions, as they may pose higher money laundering risks;

g) Transaction monitoring and pattern analysis: Tools and models that detect unusual or suspicious transaction patterns;

h) Cross-border transactions: Information on transactions crossing international borders to identify potential cross-border money laundering; and

i) Compliance data: Records related to compliance efforts, including internal policies, training, and audit reports.

2. Are there specific tools, mechanisms, or models from other jurisdictions that could be incorporated into Canadian legislation to support greater information sharing?

The following tools and mechanisms should be considered:

a) Secure information sharing platforms: Implementing secure platforms where reporting entities can share information while adhering to data protection standards. These platforms (including the Canadian Cyber Threat Exchange) have greatly assisted sharing cyber threat information in the cybersecurity realm;

b) Centralized Databases: Establishing a central repository to collect and analyze information from various reporting entities, enhancing coordination and efficiency;

c) Whistleblower Protections: Encouraging individuals in reporting entities to come forward with valuable information through whistleblower protection programs;

d) Regtech Solutions: Embracing regulatory technology (Regtech) solutions to automate compliance processes and improve data analysis.

3. What guardrails would best protect personal information while allowing for additional information to be exchanged between organizations?

Canada should consider the following principles (some are core principles of federal and provincial privacy laws):

a) Anonymization and encryption: Anonymizing and encrypting personal data before sharing it to prevent direct identification;

b) Data minimization: Sharing only the minimum necessary information required for anti-money laundering and counter-terrorist financing purposes;

c) Clear purpose and consent: Establishing clear purposes for data sharing and obtaining explicit consent from individuals when required;

d) Strong data protection regulations: Implementing robust data protection laws and regulations to safeguard personal information. The consultation paper correctly identifies the need to amend PIPEDA in this context; and

e) Access controls and audit trails: Implementing access controls to limit information access to authorized personnel and maintaining audit trails to track data usage.

4. How can the government enhance two-way information sharing between FINTRAC and the private sector?

Sharing between FINTRAC and the private sector would be facilitated using secure communication channels and regular consultations with reporting entities.

5. Are there additional guidance or strategic intelligence products FINTRAC should look to provide to reporting entities and the public?

FINTRAC should consider regular reporting on emerging threats and trends and sector-specific guidance to assist reporting entities in understanding and meeting their compliance obligations.

6. Should the government create and maintain a database of politically exposed persons (PEPs), heads of international organizations (HIOs), and their family members and close associates?

These databases have proven to be effective tools in other jurisdictions and would be of assistance in this context. We note FINTRAC issued guidance on PEPs of reporting entities, effective June 1, 2021.

7. How could the government improve outreach and engagement with the non-profit sector on AML/ATF matters?

Engagement between the CRA and the charitable and not-for-profit sector have not been productive to date. Large roundtable meetings in January 2016 and February 2020 with diverse charities operating internationally (including in conflict areas) and the CRA Review and Analysis Division (RAD) on AML/ATF matters yielded no results.

Significant advocacy was required to achieve recent amendments in Bill C-41, *An Act to amend the Criminal Code and to make consequential amendments to other Acts* (now S.C. 2023, c. 14). This legislation enables, in part, Canadian charities to offer humanitarian aid in Afghanistan and other areas controlled by terrorist groups.

Notwithstanding the important achievements in Bill C-41, it does not go far enough to adequately respond to the concerns of the CBA Sections and others over the last two decades about charities and not-for-profits operating effectively without running afoul of Canada's overreaching AML/ATF legislation.

While late, Finance Canada's March 2023 Updated National Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada (National Assessment) is a welcome response to the comments made by the sector since its initial publication in 2015.

Still, the updated National Assessment continues to focus excessively on organizations connected to racialized communities, such as the Muslim community, resulting in a disproportionate number of Muslim charities being audited and having their charitable status revoked. More transparency is required on how the National Assessment is compiled and how it is applied by RAD's audits of charities (Muslim charities in particular).

Future outreach and engagement with the not-for-profit sector on AML/ATF should be informed by the experience in the UK, US and New Zealand. We need to ensure an open dialogue and a greater understanding of the obstacles faced by charities operating internationally to develop a balanced approach of AML/ATF compliance and effective charitable activities.

E. CHAPTER 9 (National and Economic Security)

1. Should FINTRAC take a more proactive role in combatting sanctions evasion?

Several amendments to the PCMLTFA and Canada's sanctions laws were recently passed.[14] Prior to these amendments, the PCMLTFA required regulated entities to report matches with terrorist sanctions lists under the *Criminal Code* and the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

The amended PCMLTFA will now also require regulated entities to report to FINTRAC where a reporting obligation arise under the *Special Economic Measures Act* and the *Justice for Victims of Corrupt Foreign Officials Act* (Sergei Magnitsky Law). Additionally, the amendments to the *Special Economic Measures Act* enable the Minister of Foreign Affairs to disclose to FINTRAC "any information that is relevant to the making, administration or enforcement" of the sanctions regulations, or seizure orders enacted under the sanctions laws. Amendments to the PCMLTFA enable FINTRAC to share information with the Minister of Foreign Affairs.

These amendments establish the foundation for increased collaboration between Global Affairs Canada (GAC) and FINTRAC on enforcement of sanctions laws.

The CBA International Law Section has engaged extensively with GAC since February 2022, when Russia invaded Ukraine, yet there remains significant confusion and lack of clarity on Canada's sanctions laws. While we support an increased role for FINTRAC for sanctions evasion, we stress the need for clarity, transparency and guidance on Canada's sanctions laws. We urge that further collaboration between GAC and FINTRAC be harmonized and ensure consistency in the understanding and application of Canada's sanctions laws.

III. CONCLUSION

We appreciate the opportunity to comment on how to improve Canada's anti-money laundering and anti-terrorist financing regime. We trust that our comments are helpful and would be pleased to assist as we are able.

14 *C-47, Budget Implementation Act, 2023, No. 1*