Submission to the Department Finance's
Consultation on Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

Submitted by the
International Civil Liberties Monitoring Group

August 4, 2023

International Civil Liberties Monitoring Group
#210-4 Florence Street, Ottawa, ON, K2P 0W7
national.coordination@iclmg.ca | http://iclmg.ca
(613) 241-5298

We welcome the opportunity to provide feedback in the government's efforts to review and update the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA).

The International Civil Liberties Monitoring Group is a pan-Canadian coalition of 44 civil society organizations founded in 2002 to defend civil liberties in Canada in the context of Canada's anti-terrorism laws, policies and activities and the global "war on terror." Our members are from a wide array of sectors, representing human rights, civil liberties, legal, faith based, labour, international assistance and environmental groups, among others.

Our interest and expertise on this issue is in regard to Canada's anti-terrorist financing (ATF) policies, and specifically their impacts on civil liberties and the activities of civil society organizations.

Below we have provided feedback on key areas of the consultation document that relate to our mandate and the work of our coalition, and that we hope will prove useful and meaningful as the Department of Finance moves forward with this review. We would be happy to discuss our concerns and recommendations further at any time.

Before addressing specific questions from the consultation document, we believe that it is important to place our comments in context with regards to Canada's overall anti-terrorism regime, as well as to raise some issues nor covered in the consultation document.

First, any evaluation of the PCMLTFA and the broader anti terrorism financing (ATF) regime around it must be considered in the broader context of Canada's approach to countering terrorism since 2001, and the adoption of the first *Anti-terrorism Act* (ATA).

The September 11, 2001, terrorist attacks in the United States gave grounds for the Canadian government's creation of broad anti-terrorism policies which granted various departments, and particularly security agencies, sweeping new powers. Over the past two decades, these powers have been criticized for undermining rights, increasing secrecy, and broadening state surveillance programs. Researchers have also documented their use to target specific political or religious groups, particularly the Muslim community, along with Indigenous and other racialized communities. This includes the expansion of Canada's Anti-Money Laundering (AML) regime to include anti-terrorist financing (AML/ATF) with the passage of the *Anti-terrorism Act* (ATA). This bill modified Canada's *Proceeds of Crime (Money Laundering) Act* to include terrorist financing, creating the new *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA).

To effectively enforce these new ATF regulations, the government created the Financial Transactions and Reports Analysis Centre (FINTRAC), granted new powers to various national security and financial entities, including Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), the Canada Border Services Agency (CBSA) and the Canada Revenue Agency (CRA), and created coordinating bodies to facilitate intelligence gathering and sharing. This also included increased information and intelligence sharing, and harmonization of

policies, with foreign governments and agencies as well as multilateral international organizations.

Over the course of the ensuing two decades, anti-terrorism legislation and policies, including the ATF regime, have created an environment conducive to surveillance; restrictions of civil liberties and human rights; and violations of *Charter* rights, including freedom of expression, freedom of association, due process rights, privacy rights, and the right to non-discrimination. In particular, we have documented occurrences of systemic racism, racial profiling, targeting and bias towards Muslim Canadians, as well as other racialized communities, and significant impacts on the work of international assistance and humanitarian organizations.

Finally, like many federal agencies involved in national security, Canada's ATF regime – including the implementation of the PCMLTFA – has long operated without independent review or oversight. The nature of this work also means that much of what is carried out is kept secret. We would also argue that there have been little to no proactive efforts towards transparency with civil society organizations or with the public. The creation of the National Security and Intelligence Committee of Parliamentarians (NSICOP) in 2018 and the National Security and Intelligence Review Agency (NSIRA) in 2019 has presented new opportunities for independent review. For instance, NSIRA has announced it is reviewing FINTRAC's information sharing activities, as well as the CRA's national security related activities. However, the impact of Canada's ATF regime remains under-studied and should be the subject of greater oversight and review.

It is also disappointing that the consultation does not engage more with concerns around the protection of civil liberties, human rights and even Charter rights in regard to the PCMLTFA, FINTRAC and the ATF regime more broadly.

For example, while the consultation document explicitly engages multiple times with issues of privacy and section 8 *Charter* rights, it does not engage with concerns around impacts on freedom of expression, freedom of assembly or freedom of association (s. 2), or equality rights (s. 15). Each of these rights have been amply demonstrated to be impacted by, for example, surveillance and other privacy infringing activities, as well as issues of racial, religious and political profiling in the carrying out of intelligence and law enforcement activities. Examples of specific areas where these issues have arisen are included below, specifically regarding the impact on Muslim charities in Canada and the activities of international assistance organizations.

This concern is not limited to domestic law; Canada also has international obligations, both under treaties and conventions, but also under international human rights law. As the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (SR) has documented, ATF activities also implicate[1]:

[1] https://www.ohchr.org/sites/default/files/2022-06/2022-06-13-SRCT-HR-CFT-Position-Paper.pdf

- Freedom of opinion and expression
- Freedom of peaceful assembly and association
- Freedom of religion or belief
- Right of minorities
- Right to enjoy property, including through financial access
- Rights to education and work
- Equal rights of women
- Right to freedom from interference with privacy, family, or home, or unlawful attacks on one's honor and reputation
- Rights to freedom of movement and nationality
- Right of every citizen to take part in public affairs, and associated public consultation rights
- Due process and procedural rights, including the right to fair trial, the presumption of innocence, the right to appeal, and a right to effective protection by the courts
- Right to an effective remedy

Chapter 3 – Federal, Provincial, and Territorial Collaboration

Part II – Operational Effectiveness

We would raise an overall concern with the premise of this section of the consultation. The description of this section states that:

> By certain metrics, Canada's AML/ATF Regime struggles to be effective. For instance, federal money laundering and terrorist financing charges, convictions, and forfeiture of proceeds of crime have all decreased over the past decade, which is not in line with Canada's risk profile. Both the FATF [Financial Action Task Force] and the Cullen Commission criticized the AML/ATF Regime for its lack of operational effectiveness in these areas.

We are concerned that the measure of success in ATF is based on the level of prosecution in relation to Canada's "risk profile." As explained in the 2023 National Inherent Risk Assessment (NIRA),[2] the risk profile is based upon inherent risk before mitigation measures. There is strong regulation and mitigation in place across most sectors – especially the NPO and charitable sector – in order to counter potential terrorist financing. To argue for greater operational powers based on inherent risk without taking into account existing mitigation powers raises concerns of potential overreach. Moreover, in analyzing the profiles of the entities viewed as posing a terrorist financing risk in Canada, most are described as having "limited" fundraising activity, having "low" capacity, as having "greatly declined", as being "small" and "less

[2] https://www.canada.ca/content/dam/fin/programs-programmes/fsp-psf/nira-neri/nira-neri-eng.pdf [NIRA 2023]

organized" than in 2015, and having "diminished." This therefore does not support the argument that more operational powers are needed, and could instead indicate that current powers – at least in regard to ATF – are sufficient.

Further, as we discuss in other sections, we have deep concerns around how the government's risk assessment is carried, both in how it has unduly singled out Muslim, Arab and other racialized communities as being a focus of "risk," as well as the lack of involvement of the broader NPO sector in assessing risks.

Our primary recommendations for this section are that, before considering greater operational powers:

- more analysis of the problem to be addressed be carried out with stronger definition of "effectiveness" in Canada's ATF activities
- that the Department of Finance and other government agencies re-evaluate and reform the risk assessment process to be more transparent, accountable and inclusive

Chapter 4 – Criminal Justice Measures to Combat Money Laundering and Terrorist Financing

4.4 – Access to Subscriber Information under the *Criminal Code*

- Should the Criminal Code be amended to include an order for subscriber information?

We have serious reservations and would oppose the creation of an order for subscriber information in the Criminal Code.

As mentioned in the consultation document, the Spencer decision has been fundamental in interpreting the privacy rights associated with subscriber information held by Internet service providers.

In 2016, the federal government held consultations on Canada's national security laws. In the resulting summary of submissions,[3] it was clear that one of the most unifying and resounding concerns was around proposals for easier access to BSI:

> *Perhaps the most revealing result of the online consultations is that seven in 10 responses consider their Basic Subscriber Information (BSI) – such as their name, home address, phone number and email address – to be as private as the actual contents of their emails, personal diary and their medical and financial records.*

[3] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-nsc-wwlr/index-en.aspx

Almost half (48%) said BSI should only be provided in "limited circumstances" and with judicial approval, and about one in six (17%) said it should only be available to law enforcement in emergency circumstances, and even then only with a judicial warrant. The principal concern about revealing someone's BSI is that it could be used for location tracking or to access even more online information about that person.

In our organization's submission to that consultation, we also opposed loosening access to BSI, writing that:

"There is a reason the Spencer decision limited access to BSI: to protect Canadians' privacy rights. That ruling must be respected and police and national security agencies should obtain a warrant at all times when they want BSI, even when the telecommunications companies would otherwise give it voluntarily. In some true emergency situations (i.e., if a life is in danger or a crime is about to be committed), the criminal code already allows police to access BSI without a warrant."[4]

At the time, several privacy, internet and human rights experts pointed out that the consultation documents failed to make the case that such indiscriminate powers are needed, and relied on long standing claims that current access mechanisms are "inconsistent and slow." We see no different or new information or evidence presented in this current consultation; indeed, the primary argument seems once again to be concerns about the speed at which information can be obtained.

Finally, we are concerned that while this proposal is being presented in regards to ML and TF, that it will not be restricted to this purpose. For example, similar proposals recently appeared in the Online Harms consultation from Heritage Canada. It is also unacceptable that this proposal, soundly rejected in every previous consultation where it came up, would once again be raised in this context.

4.9 – Intelligence and Evidence

- How could the government improve the legislative framework governing the protection and use of sensitive intelligence and information during court proceedings in relation to money laundering and terrorist financing?
- What would be the benefits to such reforms?
- What would be the drawbacks?

While recognizing that terrorist financing cases can be complex, we do not believe that sufficient information has been presented to justify further changes to rules on the use of intelligence in court proceedings. This is especially true in regard to further reducing the

[4] https://iclmg.ca/investigative-capabilities-in-a-digital-world/

amount of government disclosure required in either criminal or civil cases. The current system, using national security and international relations as reason to keep information, intelligence and evidence secret and unavailable to defendants, is rooted in the concept of "state secrets" which is already prejudicial against defendants in several ways.

In criminal cases, it is understood that any system that denies direct access to the evidence presented against a defendant is a violation of the right to a fair and equitable trial. Moreover, once state secrets are invoked under s. 38, the case automatically changes venues to Federal Court (even if it was in Superior Court); this, despite the fact that the judge in a criminal case is the best suited to judge the relevance of evidence to be used against the accused. Because of the regulations and the secrecy, judges can accept intelligence, hearsay and other information that is normally inadmissible without the defendant ever knowing. This goes so far as to include information obtained under torture. Further, the minister in question controls the evidence. They have no obligation to share all the evidence – including any exculpatory evidence.

For example, in the cases of Adil Charkaoui and Mohamed Harkat, we know that CSIS destroyed original evidence, and entered into evidence only summaries. This falls far short of full disclosure. This system is inherently unfair and must be reviewed.

A defendant should at all times have access to the evidence used against them in order to mount an adequate defence and to ensure a fair and just trial.

Nor are these concerns addressed by the use of special advocates; we argue that – as it is the case in the security certificate regime – they cannot repair a system that completely goes against the principles of fundamental justice and the right to a fair and open trial. Again, a defendant should at all times have access to the evidence used against them in order to mount an adequate defense and to ensure a fair and just trial.

Finally, the framing of this questions also ignores the multitude of ways that government agencies and financial institutions already use intelligence, outside of formal legal proceedings, to counter terrorist financing. For example, the CRA's use of intelligence to investigate, audit and penalize charitable organizations; CSIS' use of intelligence when carrying out threat disruption activities in relation to terrorist financing; the government's use of intelligence when issuing a certificate under the *Charities Registration (Security Information) Act* as well as when determining whether to add an entity to the Terrorist Entities List; and private financial institutions' use of intelligence to de-risk and de-bank clients over suspicions of terrorist financing.

As we more thoroughly explore in other sections of this submission, the reliance on intelligence can have significant negative repercussions. This is particularly true in relation to reliance on information and intelligence that perpetuates systemic discrimination and Islamophobia, as well as intelligence regarding the operations of international development and humanitarian organization.

Chapter 6 – Information Sharing
6.1 – Private-to-Private Information Sharing

The government is seeking views on the potential expansion of a framework for private-to-private information sharing for AML/ATF purposes, and is seeking feedback on the following:

- 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?
- Are there specific tools, mechanisms, or models from other jurisdictions that could be incorporated into Canadian legislation to support greater information sharing?
- What guardrails would best protect personal information while allowing for additional information to be exchanged between organizations?
- Are there opportunities to leverage technology to enhance information while protecting personal information?

Once again, we are concerned that little detail is given in the consultation document regarding the necessity to increase information sharing between private entities, especially given the clear and heightened risks that sharing between private entities can entail, as compared to public-to-public sharing and even sharing between private and public entities.

While it may be the reality that individuals are able to access a broader range of financial services and that this could be employed by those who wish to engage in terrorist financing could avail themselves of this, there is no evidence presented that Canadian financial institutions are actually seeing increased difficulties in tracking TF crimes, nor that existing powers are insufficient or that new powers of private-to-private information sharing is needed.

While the Financial Action Task Force (FATF) is cited to justify the need for more private-to-private information sharing, the task force's own evaluation of Canada does not seem to support the need for greater private to private information sharing.

For example, the FATF identifies recommendations 13, 14, 16 and 17 as being those which rely on private sector information sharing. In the FATF's 2021 updated evaluation of Canada, it found the country to be largely compliant on 13 and 16 and compliant on 14 and 17 and does not mention the need for greater private sector information sharing (nor is this raised in the more detailed 2016 evaluation of Canada). [5]

[5] https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fur-canada-2021.html

Moreover, in its 2017 guidance on private sector information sharing, the FATF highlighted the high-risk level of information sharing among private entities, writing:

> 73. However, such information sharing can also raise a range of public policy concerns about how the information will be used (or misused), including unfair commercial practices, encouraging de-risking and financial exclusion, potentially breaching STR confidentiality and increased risk of tipping-off, customer confidentiality, data protection and privacy, financial institution secrecy, as well as the general information sharing challenges described in the earlier part of this guidance.
>
> 74. For example, sharing of customer information between financial institutions could potentially raise competition concerns resulting from selective sharing of information with only a small group of participants. De-risking and defensive STR filing behaviour may be exacerbated, e.g., if financial institutions feel obliged to file an STR on a customer simply because they have learnt that other financial institutions have done so (and without conducting their own internal investigations). Overreliance on a system of sharing of suspicious information or a common platform could potentially lead to moral hazard where a financial institution would regard a potentially suspicious customer as suspicious before proper due diligence is done, and hence preventing the customer from accessing the entire financial system. [6]

As identified in the section on de-risking below, we already see some of these negative impacts playing out, even without greater information sharing powers between private entities. We do not believe that greater information sharing on the basis of terrorist financing suspicions is warranted, nor that it could be appropriately mitigated in a way that eliminates the risk to fundamental rights.

More recent FATF reports have lauded the possible technological advances of "data pooling" and "collaborative analytics", whereby by financial institutions share information into a collective "pool" which is then analyzed using algorithms to monitor for money laundering and/or terrorist financing activity.[7] However, these proposals raise significant concerns regarding privacy; accountability, transparency and explainability; and bias. For example, es discussed in other sections, current concerns about bias in which clients are flagged as at risk for terrorist financing by banks and government agencies would result in biased algorithms that would further entrench systemic issues. In the same FATF report, financial institutions reported that "data quality" was a key problem even in pilot projects, where the quality and accuracy of data provided by financial institutions was poor or out-of-date, and that it was difficult to

[6] https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html
[7] https://www.fatf-gafi.org/en/publications/Digitaltransformation/Data-pooling-collaborative-analytics-data-protection.html

ensure the accuracy of data being used, especially after the implementation of encryption, which is essential to privacy protections. It is clear that the risks associated with data sharing for this kind of "Big Data Analytics" will result in significant harm, much of which would be hidden behind "unexplainable" algorithms.

Finally, we would disagree that *PIPEDA* does not already provide an adequate, regulated avenue for sharing information between private entities. Paragraph 7(3)(d.1) reads:

> 7(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is
>
> > (d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;

The threshold of "reasonable" is appropriate, and the scope of "a contravention of the laws of Canada or a province" is broad enough to cover acts of terrorist financing. If the information is not pertinent to a contravention that "has been, is being or is about to be committed" it is not concrete enough to justify sharing among private entities.

6.2 – Public-to-Private Information Sharing

Sharing Information Between FINTRAC and Reporting Entities

- How can the government enhance two-way information sharing between FINTRAC and the private sector?
- Should FINTRAC be provided with additional powers to request information from reporting entities? If so, what kinds of information and why?
- What sort of additional information should FINTRAC be able to provide to reporting entities regarding compliance and/or intelligence?
- Are there additional guidance or strategic intelligence products FINTRAC should look to provide to reporting entities and the public?

In discussing "Public-to-Private" information sharing, it is important to be very specific about what is being discussed. In fact, there are two areas being addressed in this section, "Public-to-Private" whereby the government shares information with private entities, and "Private-to-Public", whereby private entities share information with the government. Each raises specific concerns and must be addressed separately.

<u>"Public-to-private"</u>

While we agree that it is important for the government to be in conversation with private entities (both for profit and nonprofit organizations), the information shared with private entities must remain limited in order to prevent misuse or abuse of shared information. As noted in the consultation document, FINTRAC already have the legislated ability to engage in public-private partnerships, including sharing of information, and has done so successfully in various areas. FINTRAC also engages with the private sector through the Advisory Committee on Money Laundering and Terrorist Financing (ACMLTF). From the available information, it does not appear that there is any need for changes to allow greater "public-to-private" information sharing, and certainly no need that would outweigh the risks.

"Private-to-public"

Similar to the previous section, we do not believe that substantial changes need to be made to the information sharing regime to increase information shared by private entities with public institutions, including FINTRAC. Beyond the partnerships and the ACMLTF already noted, sufficient powers already exist for both private entities to share information with FINTRAC, and for FINTRAC to request information from those entities, including in both PIPEDA and in the PCMLTFA.

However, limited changes around information that FINTRAC can request from reporting entities may be warranted for the purpose of being able to verify and/or clarify information provided to FINTRAC. As noted in the consultation document, FINTRAC is currently limited to requesting information that is "required" from a reporting entity (PCMLTFA 54(1.1)). However, it cannot request information in order to clarify or to hep verify information provided. We have seen in our work how inaccurate and unverified information can have negative consequences in regard to profiling and the protection of civil liberties and human rights. Therefore, a provision allowing FINTRAC to request specific information in response to a submitted report from a reporting entity, for the sole purpose of clarifying or verifying the information in the report could be acceptable if it remains narrow and limited. Provisions should be put in place for the disposal of any extraneous information provided by a reporting entity in its response, as well as requiring FINTRAC to document any request for clarifying information and the reasons for it.

Under no condition should FINTRAC be granted broad powers to request information from reporting entities for the vague reason of "analysis of suspected terrorist financing." This would grant vast new surveillance powers that would put at risk the privacy and other rights of clients of broad swaths of the public who are clients of reporting entities. This is especially true due to vast information sharing powers within government, where information collected by FINTRAC can be shared with nearly twenty other government agencies.

Non-Profit Sector Outreach

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

Engagement with the non-profit sector on addressing ATF is essential to ensuring that government measures are assessed for their impact on important areas ranging from privacy rights, the rights to freedom of association and expression, due process rights and equality/non-discrimination. It is disappointing that the consultation document does not engage with this question more, given the existing documentation and research on the impact of Canadian and international ATF measures on the sector.

This is especially true given that there have been significant examples in just the past two years of the harm caused by the government's lack of engagement with NPOs and civil society more broadly. This includes groundbreaking reports on systemic Islamophobia in Canada's ATF operations, as well as the ban on Canadian organizations providing assistance to areas under the control of terrorist entities, exemplified by the case of Afghanistan. Neither of these issues appeared suddenly in the past two years; they have been consistently raised and identified as highly problematic aspects of Canada's ATF regime. With more constructive and concrete engagement with the NPO sector, fixes could have been proposed and implemented to address these issues and minimize the harm they have caused. We hope that going forward, the government will implement – through policy and legislation – meaningful approaches to consulting with the sector and implementing reforms.

Before discussing what engagement with the sector should look like, it is important to highlight what it should not look like. While the government must create opportunities for the NPO sector to engage in ways to concretely reduce violence and crime that impact their communities, other examples of similar government outreach have led to troubling results. It is crucial that engagement and outreach is not predicated on the idea of collecting intelligence or recruiting organizations into the fight against ATF. While guidance on how to minimize risk may be helpful, actions that even indirectly lead to surveillance of community members is unacceptable. For example, we have been greatly concerned by government and law enforcement agencies use of violence reduction partnerships to further counter-radicalization efforts, as well as CSIS "outreach" visits that are motivated by enlisting community members to inform on their neighbors and associates.

With that in mind, there are some key areas/ways that the government could improve outreach and engagement with the sector in regard to ATF:

Guidance on risk reduction: non-profit organizations with social good mandates often already take steps to mitigate risks that may have negative impacts on their work, membership and community at large. Better tailored guidance to the NPO sector regarding how they can mitigate ATF risks would be beneficial

Assessments and evaluations: As recommended by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering

terrorism (SR) and expanded on further in section 7 below, NPOs should be involved in the assessment and evaluation of ATF laws, policies and regulations.[8] This includes the National Inherent Risk Assessment. Unfortunately, we have seen little to no concrete engagement with NPOs in this area, including in regard to the NPO sectoral assessment referred to in the 2023 NIRA. The government should create venues for meaningful engagement and feedback from the sector. Any such engagement must go beyond existing frameworks; for example, while the government has involved NPOs and civil society in its National Security Transparency Advisory Committee, despite the important recommendations made it is unclear whether its work has been integrated by Public Safety Canada or had concrete impact on transparency issues at the various national security agencies.

One option would be to create a NPO advisory body similar to the Advisory Committee on Money Laundering and Terrorist Financing (ACMLTF). Some may recommend integrating NPOs into the existing Advisory Committee; while we would agree that the absence of NPOs from this body is glaring and demonstrative of broader concerns with the AML/ATF landscape in Canada, NPOs experience specific challenges and can provide specialized feedback that should be approached separately.

Training and expertise: FINTRAC and other agencies working on ATF should also engage with the NPO sector in order to receive training and engage sector experts in regard to human rights, diversity, systemic and unconscious bias, and the realities of how NPOs operate in various sectors and areas. While it is unclear what the situation at FINTRAC is, recent testimony to the Senate revealed that training for CRA staff working on ATF on the issues was not only minimal, but optional. This is unacceptable and should be a priority for internal reform.

Each of these areas should be addressed not just policy reform, but legislative changes that set requirements for engagement, assessments and training.

[8] https://www.ohchr.org/sites/default/files/2022-06/2022-06-13-SRCT-HR-CFT-Position-Paper.pdf

6.3 – Public-to-Public Information Sharing

Targeted Information Sharing Between Operational Regime Partners and Law Enforcement

- How can the government improve the timely access to targeted information amongst operational partners in Canada's AML/ATF Regime to increase money laundering charges, prosecutions and convictions, and asset forfeiture results in Canada?
- Does this proposal raise any privacy considerations?

Enhancing Financial Intelligence Disclosures

- How can the government facilitate more timely, accessible, and actionable financial intelligence disclosures from FINTRAC to law enforcement and national security agencies?
- Should the government amend the PCMLTFA to expand the list of disclosure recipients to which FINTRAC discloses designated information when legislative thresholds are met?
- Which organizations/agencies should be added to the list of disclosure recipients?
- Does this proposal raise any privacy considerations?

We would not support changes to increase access to targeted information, to facilitate the release of financial disclosure materials or in order to expand the list of organizations to whom such disclosures can be sent.

Unlike other sections where minimal information is provided to support possible expansions of the current regime, no evidence is provided whatsoever to support the proposals in this section. Further, it largely ignores the already substantial powers that FINTRAC and AML/ATF regime partners have that allows them to access as well as to disclose information required to carry out their work.

In terms of access, the consultation document itself states that "Canada's legislative framework allows the AML/ATF Regime's core operational partners (i.e., FINTRAC, the RCMP, CBSA, CSIS, and the CRA) to obtain the information they need to support their individual mandates." It is unclear why there are concerns about "timeliness" and no information is provided regarding the impacts of any delays, making it impossible to adequately assess the issue. We therefore would not support changes to this effect, especially given that efforts to improve timeliness often result in reducing privacy and rights safeguards, and reducing oversight, review, transparency and accountability.

Regarding disclosure, once again no information is provided in support of the suggestion to expand the number of "government departments and agencies authorized to receive FINTRAC disclosures."

The consultation document makes clear that FINTRAC can disclose financial intelligence to designated recipients based on the relatively low threshold of "reasonable grounds to suspect" that information would be relevant to terrorist financing investigations or threats to the security of Canada. Sections 54(1)(c), 55(3), 55.1 and 56.1 of the PCMLTFA clearly lay out these powers, and the broad array of law enforcement and government agencies to which FINTRAC may disclose information.

Further, FINTRAC is one of 17 listed entities under the *Security of Canada Information Disclosure Act* (SCIDA).[9] This means that any government agency may disclose information to FINTRAC if they are satisfied that "the disclosure will contribute to the exercise of the recipient institution's jurisdiction, or the carrying out of its responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada." The provisions of SCIDA also mean that FINTRAC may disclose information to any of the 16 other listed entities for those same reasons.

We have raised significant concerns[10] already regarding the provisions of SCIDA, including the low threshold of a department only needing to be "satisfied" that the information they are sharing is "relevant" to the work of the agency to which the disclosure is being made, as well as the overly broad nature of the Act's definition of "*activity that undermines the security of Canada."*

Far from granting FINTRAC more powers of disclosure, we would reiterate here the need to review information sharing provisions and restrict the disclosure powers granted under SCIDA.

Finally, the consultation document does not address FINTRAC's sharing of information with foreign entities.

Under section 56.1 of the PCMLTFA, the Minister of Finance or, with the Minister's approval, FINTRAC, to enter into an information sharing agreement with a foreign entity "that has powers and duties similar to those of the Centre" if they have "reasonable grounds to suspect" that the information "would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, or an offence that is substantially similar to either offence."

This is an incredibly broad provision for information sharing with foreign governments, agencies and international organizations.

[9] https://laws-lois.justice.gc.ca/eng/acts/S-6.9/
[10] https://iclmg.ca/issues/bill-c-59-the-national-security-act-of-2017/bill-c-59s-changes-to-c-51/

While FINTRAC has a fairly limited scope, agencies carrying out similar work in foreign jurisdictions may have a much broader scope, possibly combining intelligence gathering, monitoring and law enforcement, and even going beyond a financial crimes mandate. Regardless, there are no provisions in the PCMLTFA as to what must be in such agreements, nor for the minister or agency to seek out assurances regarding how the information disclosed by FINTRAC is used or even shared further with other agencies or other governments.

This is deeply worrisome given the history of information sharing being misused an abused in the name of "counter-terrorism" to support horrendous human rights violations.

While this is partially mitigated by the issuance of a directive by the Minister of Finance under the *Avoiding Complicity in Mistreatment by Foreign Entities Act* (ACMFEA)[11] to regulate the disclosure or request of information from foreign entities that may result in mistreatment, more safeguards must be put in place.

Firstly, FINTRAC should be added as one the agencies where a directive under the ACMFEA is required. The degree of information sharing the FINTRAC engages in necessitates an obligatory directive; under the current law, a future government could repeal the existing directive and essentially eliminate any restrictions on FINTRAC's information sharing with foreign entities.

While including FINTRAC as one of the required entities in the ADCMFEA would address some concerns, the most effective solution would be to integrate safeguards regarding FINTRAC's information sharing into the PCMLTFA.

We therefore recommend that government amend the ACMFEA to explicitly include FINTRAC, and that the government amend section 56 of the PCMLTFA to include more specific requirements and rules around both international information sharing agreements, and the sharing or requesting of information itself.

Part III – PCMLTFA Legislative and Regulatory Framework

Chapter 7 – Scope and Obligations of AML/ATF Framework

7.1 – Review Existing Reporting Entities
Virtual Currency, Digital Assets, and Technology-Enabled Finance

- Are there money laundering and terrorist financing risks posed by new financial technologies that are insufficiently covered or mitigated by the AML/ATF framework?
- What legislative and regulatory remedies could be used to address the risks posed by new FinTech products or services (e.g., Anonymity Enhancing Coins (AEC) / PrivacyCoins, crypto-mixers, DeFi)?

This is a new and emerging field that requires more study, and we would caution against rushing to regulate before the implications of such regulation is more fully discussed and consulted upon.

As the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (SR) has reported,[12] in many jurisdictions have rushed to regulate the virtual currencies, digital assets, etc., based on the perceived vulnerabilities of new technologies that has exaggerated the level of threat posed.

This is despite limited empirical evidence to date regarding the actual TF threat posed by new financial technology, especially in regard to the non-profit sector, but also across sectors more generally. As she writes:

> "To date, however, there is still only a limited body of evidence of the empirical threats posed by these new technologies. Although there have been discrete instances identified where designated terrorist groups have misused virtual assets and online exchanges and wallets, the exact extent of misuse of virtual assets and new payment. Existing documentation of virtual asset misuse typically focuses on money laundering, fraud, and theft broadly speaking; where terrorist financing is referenced, it is often not disaggregated from broader money laundering and financial crime cases."[13]

We would echo the Special Rapporteur's call for governments to avoid overregulation of these technologies and for government responses to be proportionate to the terrorism financing vulnerabilities identified. Importantly, and as we have argued, she also highlights the need for any assessments to be published publicly – including empirical evidence – and for proposed responses to be subject to open consultation with all sectors, including civil society groups.

It is important to recognize not only that there can be downstream negative impacts of any rushed regulation, but that these new technologies have been demonstrated to provide net benefits to civil society groups and to humanitarian efforts internationally. This includes providing aid in conflict regions with limited access to formal banking institutions, helping human rights defenders circumvent authoritarian governments, advancing financial inclusion, ending poverty and promoting economic growth.

While these are some of the direct impacts, regulating new technologies in the TF space also raise the same concerns as we see in the more traditional ATF space. For example, in both areas

[12] https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/activities/2023-06-09-CFT-New-Payment-Tech-Position-Paper.pdf
[13] *ibid.*

there are concerns that governments are failing to integrate human rights into ATF laws and regulations. This includes obligations under international human rights law and international humanitarian law, as well as the principles of the *International Covenant on Civil and Political Rights,* such as the right to privacy, rights to freedom of association and expression, the right to humanitarian assistance, due process rights and non-discrimination.

Finally, as we have raised in other sections, it is imperative that the government ensure non-discrimination in the implementation of any new policies in this area, particularly keeping in mind the disproportionate harms of ATF regulations to women, LGBT and gender diverse persons, and ethnic and religious minorities.

As Canada determines its approach, it must do so with restraint – particularly given the lack of both empirical evidence as well as impact assessments – and must bear in mind the domestic and international impact of the regulations it adopts and promotes.

Finally, in the same paper the SR provides some key areas that governments should consider in developing regulations around new financial technologies, including:

- **meaningful participation by civil society and affected communities** in the design, delivery, and oversight of ATF regulatory responses;
- **transparent, accessible, and readily comprehensible risk assessments** of the risks and vulnerabilities of virtual assets, crowdfunding, and other new financial technologies to terrorist financing;
- **further, concerted empirical research** on the scale and scope of the use of virtual assets and new payment technologies, and its impact on financial inclusion and other fundamental rights and freedoms;
- **human rights and gender ex ante impact assessments, due diligence, and benchmarking** in the rollout of any AFT regulatory measure;
- **unambiguous exemptions** for humanitarian and human rights organizations;
- **independent, impartial oversight and review processes** for financial technology registration procedures, de-risking, de-platforming, and other discretionary measures; and
- **consideration in any assessment of AFT compliance of human rights impacts**, including on financial inclusion and related rights, and overregulation.

Chapter 8 – Regulatory Compliance Framework

8.2 – Effective Oversight and Reporting Framework

De-Risking

- What businesses and sectors in Canada are affected by de-risking? What impact does this have on their business and operations?
- Are Canadian financial institutions de-risking certain clients? For what reason?

As pointed out in the consultation document, de-risking by financial service providers in relation to countering terrorist financing (ATF) is an important concern among non-profit and charitable organizations in Canada and internationally. In particular, recent reports have detailed how Muslim organizations in Canada have been specifically impacted by so-called "de-risking." Other reports have demonstrated how de-risking has impacted non-profit organizations more broadly and on a global scale.

While de-risking is viewed primarily as a private sector issue based on decisions made by banks and other financial service providers, a primary driver of this issue is government policy. ICLMG documented this issue in our 2021 report[14] on the impacts of Canadian AFT activities on Muslim charities in Canada. In it, we explain how Canada's whole-of-government ATF policy arose following the 9/11 attacks and, similarly to broader counter-terrorism activities, has led to a complex web of security policies that have infringed on civil liberties and human rights, increased surveillance, and stigmatized Muslim and other racialized communities in Canada. This whole of government approach means that various departments and agencies have and continues to play a role, ranging from traditional national security agencies such as CSIS, the RCMP, and Public Safety Canada, to FINTRAC and the Ministry of Finance, to less recognized partners such as the CRA, their Review and Analysis Division, and the Minister of National Revenue. This extends to federal laws, policies and guidance, including Part II.1 of the Criminal Code and both the 2015 and 2023 National Inherent Risk Assessments.

As this complex web of policies have grown, based on vague definitions of terrorism and pressure to be able to both prevent but also predict terrorism before it occurs, financial institutions decided that it was in their best interest to not only mitigate risk – as is recommended by international standards – but to avoid risk of violating these policies at all cost, particularly because of the penalties that would ensue. Such risk avoidance results in the de-risking and de-banking discussed below. In order to address this, it is imperative that the government undertake a global reassessment of both ATF as well as counterterrorism measures, involving public consultations and discussions with civil society groups and the non-profit sector (discussed further in the section on NPO engagement).

In regard to Muslim organizations in Canada, in August 2022 Steven Zhou of the National Council of Canadian Muslims reported[15] on the impact of de-risking on five major Muslim organizations in Canada, writing that,

> Major Canadian banks and various online financial services have been abruptly stopping Muslim organizations from doing any business with them.

[14] https://iclmg.ca/wp-content/uploads/2021/06/Prejudiced-Audits-ICLMG-2021.pdf
[15] https://nccm.medium.com/the-untold-story-of-de-banking-in-canadas-muslim-community-6f6b88faddef

> This includes banks telling mosques in Canada to clean out millions of dollars in reserves within weeks, as well as online fundraising services ceasing to process donations for large Muslim charities with little notice. The Muslim groups are given no reasons for why they had been dropped. Often, the two sides had been doing business for years. Some Muslim organizations have received general reasons related to "risk assessment" from the financial institution, but nothing more.

The accounts include banks suddenly refusing service after decades because it falls outside of their "risk appetite," and difficulties finding alternative banking options. Zhou documents how several major Canadian banks as well as international money processing services have engaged in de-risking without transparency, clear criteria or avenues for appeal, leading to unfair treatment and crippling the organizations in question.

Zhou's research also makes the link with the impacts on Canadian-based international NPOs, who are impacted by the global de-risking system. He profiles a major Muslim humanitarian organization in Canada that supports global relief work, documenting how they were denied service by American Express, payment processor Stripe and HSBC, all without clear reasons or transparency around the process, but clearly based on the fact that they provide aid in conflict areas facing complex human rights and sociocultural situations.

This reflects research from New York University legal clinic in Paris on the impact of de-risking on NPOs globally.[16] As they note, while banks may not treat NPOs differently than they treat other corporate clients, NPOs have suffered disproportionate restrictions on access to financial services, and that there are cases of governments instituting ATF provisions with the purpose of hindering the ability of NPOs to solicit, receive and utilize financial resources.

As summarized in the *Carters AML/ATF and Charity Law Alert No. 49*, "the Report explores the root causes: complex and multilayered regulation; the absence of an NPO's "right" to a bank account; a lack of knowledge and capacity at the bank and at the NPO; and deliberate misinformation campaigns."[17]

The recent debate around Bill C-41[18] and the impact of Canada's counter-terrorism financing laws on the provision of international assistance, including humanitarian aid, has also highlighted the sever impact of de-risking. While the central concern was the possibility of criminal charges against international NPOs and their staff, the related issue of de-risking was often raised as well. The sudden interpretation that the Criminal Code prevented these organizations from continuing to operate in Afghanistan demonstrated the lack of clarity and subjectiveness that surrounds Canada's anti-terrorism regime and which Canadian NPOs operating internationally have had to navigate for the past 20 years. It has also pushed financial

[16] https://www.hscollective.org/assets/Uploads/NYU-HSC-Report_FINAL.pdf
[17] https://www.carters.ca/pub/bulletin/charity/2021/atchylb49.pdf
[18] https://iclmg.ca/wp-content/uploads/2023/04/ICLMG-brief-re-Bill-C-41.pdf

institutions to become more risk adverse and either place additional, unnecessary safeguards that inhibit international assistance, or de-risk organizations completely. It was telling that during tesitmony at both the House of Commons and Senate, one of the primary concerns raised was whether the authorization system and/or the humanitarian exemption would apply to third party service providers, including financial institutions, and what kind of re-assurance could be given to ensure that organizations operating in Afghanistan and other complex regions would not be "de-risked." While the government has responded that third party service providers would be covered, there is still concern about how this will be conveyed, and whether this party providers will feel reassured.

More research is required in the Canadian context in order to collect empirical data of the impact of de-risking, but it is clear that de-risking is happening in Canada, reflects the international trend around de-risking impacting NPOs and particularly international and Muslim-led NPOs, and must be addressed by the Canadian government.

- Should the government take any action regarding de-risking? If so, what?
- What would be the benefits?
- What would be the drawbacks?

We believe there are areas in which the Canadian government should act on de-risking, both directly and indirectly.

Indirectly:

As documented in the NYU report, and as acknowledged by the FATF in their efforts to address the "unintended consequences" of ATF policies, government approaches to ATF can complicate the landscape for NPOs and lead to financial service providers taking a more risk-adverse approach to NPOs than is warranted.

As we have shown in our own research, while the Canadian government's own risk assessments on ML and TF identify the NPO sector and particularly charities as having an inherent high risk in regards terrorist financing, little public information is provided to support this assessment, making it difficult for those without access to classified information to assess what these threats are and how best to address them.[19] Further, the majority of the assessed risk continues to be in conjunction with organizations that are linked to Islam or operate in Muslim-majority regions.

We commend the updated 2023 NIRA for explicitly acknowledging that this this is an inherent risk assessment of a sector and that it is necessary to conduct a case-by-case assessment when reviewing the activities of any particular charity. However, the 2023 NIRA explicitly encourages financial service companies "to use the findings in this report to continue to inform their efforts

[19] https://iclmg.ca/wp-content/uploads/2021/06/Prejudiced-Audits-ICLMG-2021.pdf

in assessing and mitigating risks."[20] While the use of "mitigation" is better than "avoidance," we remain concerned that the overall message sent to the financial sector is to be wary of working with charities and Muslim-led organizations, or those NPOs operating in conflict or politically complex areas.

As raised above, and discussed in the NPO outreach section, more must be done by the government to ensure their own assessments, guidance and publications do not unduly promote more risk-adverse behaviour from the financial sector.

Directly:
Beyond addressing the messaging sent by government assessments, the report form NYU presents important and concrete suggestions for how government and the business sector can address the issue of de-risking, all while mitigating the risks of ML and TF. They base these suggestions on key principles of the United Nations Guiding Principles on Business and Human Rights ("UNGPs"), and they include:

- Embedding de-risking in human rights policy and due diligence processes
- Stakeholder engagement
- Alignment with compliance policies and guidance documentation
- Internal learning and cross-functional co-operation
- External communication and capacity building
- Fee differentiation and service models
- Improving access to effective remedies

Some of these are best addressed through improved guidance, others through possible regulations either via the PCMLTFA or legislation governing federally regulated industries, while others could also be addressed through amendments to the legislation (including the PCMLTFA), including mandating reporting on de-risking activities, and the creation of effective remedy processes.

Finally, as the Carters report also notes, there is an important social, political and human rights impetus to addressing this issue, given that "many organizations operating in high-risk and conflict zones do so where even nation-states are sometimes hesitant to become involved, in order to provide opportunities for many of the world's most vulnerable people to receive vital, life-sustaining programs."

[20] NIRA 2023

8.3 – Additional Preventive and Risk Mitigation Measures

Geographic and Sectoral Targeting Orders

- Should the government create a framework for Geographic and Sectoral Targeting Orders (GSTOs)?
- Would GSTOs help mitigate money laundering and terrorist financing risks in the Canadian economy?
- What parameters and checks and balances should apply to the governance of GSTOs?

While domestic geographic targeting orders may be more limited, we would be opposed to sectoral targeting in the context of ATF, given what we have already documented regarding the singling out and profiling of particular sectors in ATF activities. We do not believe that such orders would be necessary to mitigate terrorist financing, and would in fact exacerbate existing inequities in the process.

Part IV / Chapter 9 – National and Economic Security

The government is seeking views on the nature and scope of FINTRAC's role in helping to counter threats to Canada's national and economic security, and contribute to its sanctions and counter-proliferation framework:

- Should reporting requirements to FINTRAC and/or other obligations be amended to help better detect the financing of terrorist activities, including those conducted by lone actors and where transactions may be in small amounts or difficult to distinguish from activity that would otherwise appear legitimate?

While we agree with the overall concern that more must be done to address and prevent acts of violence, we disagree with the premise that further monitoring the financial activities of lone actors will achieve that goal. Multiple studies, including by the US government,[21] the FATF,[22] and even Canada's 2023 NIRA, have demonstrated that financing is neither a prime indicator, nor a prime tool, of lone actors. Moreover, the clear harm that would be caused by granting FINTRAC or other government bodies the ability to further monitor small transactions carried

[21] https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf [US 2022]
[22] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Ethnically-racially-motivated-terrorism-financing.html [FATF ERMT]

out by individuals for activities that are indistinguishable from legitimate financial transactions would outweigh any potential benefit.

Reports from Canada, the US and the FATF have noted that lone actors typically use their own funds to carry out "low sophistication" attacks, perhaps by buying firearms or other tools that may be otherwise lawful, and that the funds used are often licit[23]. As Canada's 2023 NIRA points out, "While certain entities which contribute to propagating violent ideologies are known to have conducted some forms of fundraising, there have been no clear links that such funds were used to conduct violent actions in Canada."

An FATF study of the issue found that, "Often lone-actor attacks are spontaneous and even involve tools already owned by the perpetrator (or in some cases easily accessible equipment like motor vehicles). As expenses for these attacks are low, and do not differ from normal transactions, there are often few or no red flags in the financial system and most useful financial information is only discovered through police investigations after an attack has taken place."[24]

The 2022 US National Risk Assessment reported that, "These lone actors are increasingly reliant on their own personal finances to fund an attack, effectively separating any financial connection to terrorist organizations and thus limiting the effect of certain AML/CFT measures at disrupting the financial aspects of terrorist activities."[25]

Based on these assessments, focusing on increased surveillance of individual, small scale and/or otherwise legal financial activities would seem unlikely to effectively identify lone actors' intent on carrying out violence. Moreover, such scrutiny would require a significant ramping up of financial surveillance, severely impinging on civil liberties and Charter rights, including privacy rights, due process rights, and rights to freedom of expression and association. As the UN Special Rapporteur has pointed out, ATF surveillance activities already "are particularly vulnerable to human rights abuse as they are typically covert in nature and performed by the State security apparatus, which makes it difficult for other governmental entities let alone the public to ensure accountability." Extending them even further would exacerbate the problem.

This is not to say that lone actors should be ignored, or that groups or organizations with which they are either affiliated or which inspire their violent activities do not engage in illegal financing activities that merit monitoring. While we would argue that Canada's ATF activities must be fundamentally revised in order to address significant human rights and civil liberty shortfalls, there is still a role for government to play in enforcing financial regulations and monitoring for illegal activity. But the effectiveness of doing so in order to address "lone actors" is not substantiated by currently available information.

[23] See: US 2022, FATF ERMT, NIRA 2023
[24] FATF ERMT
[25] US 2022

Instead, the threat of violence carried out by lone actors may be better reduced by addressing the worldviews, organizations and movements that inspire them. This would likely go beyond addressing financing, and as we have argued in other briefs, may not even be best addressed through counterterrorism activities, but rather through counter-narratives, education, activities to reduce hate speech and promote diversity and inclusion, and addressing the roots of social division (including socioeconomic inequality).

- Is the definition of threats to the security of Canada under the CSIS Act (which is used in the PCMLTFA) sufficient to capture the range of illicit financing activities that could compromise Canada's economic integrity and prosperity?
- Should businesses with obligations under the PCMLTFA be required to report to FINTRAC on suspicions of threats to the security of Canada, economic security, proliferation financing or sanctions evasion, in addition to money laundering or terrorist financing?
- Should FINTRAC's mandate be expanded to include a stronger intelligence or compliance role related to threats to the security of Canada, economic security, proliferation financing, and sanctions evasion?
- Would these authorities be better split among other government departments?
- What issues could arise from the implementation of a broader mandate?

We believe that the definition of threats to the security of Canada under the CSIS Act is sufficient for their mandate and should not be broadened. We would also be concerned if FINTRAC's mandate was further expanded to include activities that could compromise Canada's economic integrity and prosperity. Such wording is vague and overly broad. The provisions introduced this past year allowing the Minister of Finance to "direct businesses to take enhanced due diligence measures when needed for national security reasons" appears to be both sufficient and narrow enough to be effective without allowing for over-reach. It would be important to observe and monitor how these new provisions are used before considering any further expansion of FINTRAC's powers.

Further, beyond the PCMLTFA, there are provisions within PIPEDA for private entities to collect and disclose information related to national security threats to government bodies, as well as the provisions of SCIDA allowing for the disclosure of information between government departments, including FINTRAC. While we maintain concerns regarding both of the provisions, they also demonstrate that there are existing tools that can be used to collect and disclose information relating to threats to national security, which would ostensibly include economic threats (vague as that is).

Finally, we are concerned that the expansion of the definition of national security is another element of "national security creep," whereby more and more elements are added to the concept of national security and therefore responded to with a security-based response. Such "creep" results in more and more resources going to national security agencies, as opposed to

efforts at peace building, investment in domestic and international socio-economic programs or other efforts to protect human rights and civil liberties. Such investments have a proven record of improving safety and livelihoods, all while respecting fundamental rights.