Bill C-31, the *Economic Action Plan 2014 Act, No.1*

Submission to the Standing Committee on Finance (FINA)

Mr. James Rajotte, M.P
Chair, Standing Committee on Finance
Sixth Floor, 131 Queen Street
House of Commons
Ottawa ON K1A 0A6

Dear Mr. James Rajotte:

Thank you for the opportunity to present before the Standing Committee on Finance the views of the Office of the Privacy Commissioner of Canada on Bill C-31, the *Economic Action Plan 2014 Act, No.1.* As you are aware, this omnibus Bill seeks to implement several provisions of the budget, some of which are of interest for my Office. This submission will address three aspects of Bill C-31.

I. Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)

As you are aware, my Office has appeared before House and Senate Committees numerous times on the privacy implications of Canada's anti-money laundering/anti-terrorist financing regime. We support Canada's efforts to combat money laundering and terrorist financing. However, the manner in which these activities are undertaken must strike an appropriate balance between the need to combat such measures and respecting privacy rights of Canadians.

By way of background, it has long been a position of this Office to ensure that measures undertaken to keep Canada safe are done in a manner which does not sacrifice the privacy of Canadians. To that end, in our publication "*A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century*", we suggest that federal government departments apply the following four-part test to assess the proper balance between government objectives and the potential impact on privacy.

First, the test requires that there be a clearly defined **necessity** for the use of the measure, in relation to a pressing societal concern – in other words, some substantial, imminent problem that the security measure seeks to address. Second, the measure must be carefully targeted and suitably tailored, so as to be viewed as reasonably **proportionate** to the privacy rights of the individual that are being curtailed. Third, the measure should be shown to be empirically **effective** at treating the issue, and therefore clearly connected to solving the problem. Finally, the measure must be as **minimally intrusive** as possible (in other words, less intrusive avenues of investigation must have been exhausted).

The following paragraphs discuss that test in relation to the provisions of Bill C-31 related to Canada's anti-money laundering regime.

Expansion of Politically Exposed Persons

Bill C-31 broadens the requirement for financial institutions to monitor politically exposed persons – or "PEPs" – and for the first time, makes domestic PEPs subject to the Act. PEPs can include heads of state or governments, deputy minister equivalents, ambassadors, attachés, judges, generals, leaders of political parties and so on. As it stands now, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) requires reporting institutions to monitor their clients for foreign PEPs and undertake specific actions with respect to their financial activities (such as recording opening of accounts, monitoring of suspicious transactions and keeping records of the sources of funds deposited) of these clients. Bill C-31 also expands the definition of a PEP to include family members, "or a person who the person or entity knows or should reasonably know is closely associated, for personal or business reasons, with a politically exposed … person." Of note is that Bill C-31 creates a new category of PEP – a *domestic* politically exposed person – and requires the same monitoring and reporting requirements as for foreign PEPs.

We would urge the Committee to examine whether this broadening of the application of PCMLTFA to include persons who may have tangential or very tenuous connections to PEPs, is necessary, proportional and effective. This will be particularly important given that this apparently minor modification may well result in excessive monitoring on the part of private organizations, that in turn could lead to over-reporting to FINTRAC, leading to excessive information being included in FINTRAC's information holdings.

Over collection and retention

One implication of the four-part test is that an organization cannot collect or retain more information than it needs to meet its legitimate objectives. Yet, over collection has long been an issue of concern under this regime. As you are aware, section 72 of the PCMLTFA requires my Office to conduct biennial reviews of how FINTRAC protects information it receives or collects under this Act; in fact, this is the only legislated review that my Office *must* undertake. We have completed two such reviews and in both cases, we found that reporting entities submit too much information to FINTRAC.

In our 2009 report, we found that FINTRAC's acquisition of information extended beyond its legislative authority.[1] In the 2013 follow-up to that report, we determined that little progress had been made to address over reporting.[2] In both cases, we recommended that FINTRAC work with reporting entities to ensure that it does not receive information it has no authority to receive.[3] Furthermore, we recommended that FINTRAC implement front-end screening to

[1] Audit Report of the Privacy Commissioner of Canada, *Financial Transactions and Reports Analysis Centre of Canada*, 2009, page 11.
[2] Audit Report of the Privacy Commissioner of Canada, *Financial Transactions and Reports Analysis Centre of Canada*, 2013, page 7.
[3] It should be noted that the PCMLTFA allows for extensive fines, and includes the possibility of imprisonment, for failure to report certain kinds of transactions. Since neither the *Privacy Act* nor its private-sector counterpart, the *Personal Information Protection and Electronic Documents Act* (PIPEDA)

ensure that information it should not have received is expunged from its databases. However, FINTRAC is of the view that it cannot conduct such front-end screening, and that it must keep whatever information is in its databases for ten years in order to comply with the terms of the Records Disposition Authority as issued by Library and Archives Canada.

On a positive note, we are encouraged to see that C-31 introduces this very requirement: FINTRAC must now destroy information in its holdings which was either not required to be reported, or any information voluntarily provided to it "by the public that it determines, in the normal course of its activities, is not about suspicions of money laundering or the financing of terrorist activities." Furthermore, FINTRAC is required to destroy the information "within a reasonable time after the determination is made." While this requirement is in alignment with the recommendations we have made in both reviews of FINTRAC, we would like to see a specific time period prescribed for FINTRAC to cleanse its databases of extraneous information. To be privacy sensitive, this should be done as soon – and as thoroughly – as possible. Ideally, although we are aware of FINTRAC's view on this matter, we would recommend that FINTRAC screen information as it is submitted (that is, prior to being saved in their information holdings) in order to ensure not only that their databases are kept free of irrelevant information, but also that they meet their obligations to collect only that which is directly related to their activities as required by section 4 of the *Privacy Act.* In the interest of ensuring that only that which is required to be submitted, is submitted to FINTRAC, my officials have been conducting outreach activities with the Canadian Bankers Association, the Office of the Superintendent of Financial Institutions and FINTRAC to ensure that reporting institutions understand the parameters of their reporting obligations. We have also issued fact sheets in this regard.

Information Sharing

We appreciate that FINTRAC must share intelligence with its partners in order to combat terrorist financing and money laundering. In fact, the PCMLTFA allows for – and, in some cases, compels – FINTRAC to share information with the Canada Revenue Agency (CRA), the CBSA, the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment of Canada (CSEC) and police forces, among others. Bill C-31 expands the scope of what can be shared, as well as requiring FINTRAC to share information related to threats to the security of Canada not only with CSIS, as has already been the case, but also with the CBSA and appropriate police forces. Given this increased ability – and, in some cases, requirement – to share information, it is crucial that FINTRAC ensure the accuracy, relevance and currency of information it holds. We believe that more can be done in terms of clarifying to all information sharing partners what should and should not be reported to FINTRAC.

Other

Finally, there are many measures in Bill C-31 with respect to the PCMLTFA with which we do not, for the present, take issue. We note that Bill C-31 seeks to amend the PCMLTFA to, among other things, enhance the client identification, record keeping and registration requirements for financial institutions and intermediaries; and modifies information that

---

include such penalties, it is perhaps unsurprising that institutions would rather risk over-reporting than expose themselves to such a penalty under the PCMLTFA.

FINTRAC may receive, collect or disclose; and expands the circumstances in which the FINTRAC or the Canada Border Services Agency (CBSA) can, and sometimes must, disclose information received or collected under the Act. It also updates the review and appeal provisions related to cross-border currency reporting. While these specific elements of C-31 do not appear to raise privacy issues for the present, we will be interested to see how these measures unfold.

II. United States *Foreign Account Tax Compliance Act* (FATCA)

Continuing with the subject of information-sharing, Bill C-31 introduces an Agreement to implement the exchange of tax information between Canada and the United States which, we understand, resulted from discussions between Canada and the United States regarding the United States *Foreign Account Tax Compliance Act* (FATCA). FATCA requires financial institutions in countries outside of the United States, including Canada, to report certain information on accounts of a "U.S. Person" to the U.S. Internal Revenue Service (IRS). Under the Agreement, Canadian financial institutions will be required to begin due diligence procedures starting July 1, 2014, and to report information to the CRA beginning in 2015. It is our understanding that the first exchange of information between the CRA and the IRS will be in 2015. I would like to note that there is a long-established practice of information sharing between nations for the purposes of taxation enforcement. This isn't a new concept. That said, we would expect that this and all information sharing activities be undertaken in a way which respects privacy.

We are aware that some hold the view that this agreement violates section 15 of the *Canadian Charter of Rights and Freedoms* on the basis that it discriminates against Canadians based on place of birth or citizenship[4]; however, this issue is beyond the scope of my Office's mandate.

Equally beyond our scope is how foreign jurisdictions implement their own tax collecting operations. That said, if Parliament seeks to make this reporting requirement required by law, we would expect that CRA will carry out its new FATCA-related responsibilities in a manner which meets its obligations under the *Privacy Act.* Similarly, we expect private-sector organizations, such as financial institutions, that may be legally required to collect and disclose customers' personal information to CRA pursuant to FATCA, to comply with their privacy obligations under PIPEDA. These obligations include the requirement that, among other things, organizations limit the amount of personal information they collect about individuals and safeguard the personal information in their care. To that end, we would expect that education and outreach to institutions affected by this new reporting requirement, should it pass, would be crucial in ensuring that is it done in the most privacy-sensitive manner possible.

The extent to which these two elements of Bill C-31 – expanding the collection of information in the context of anti-money laundering and undertaking information-sharing with a foreign state for the purposes of enforcing a foreign law – represent a gradual expansion of scope is currently unknown. We note that when the PCMLTFA was first introduced in 2002, it had narrowly and clearly defined reporting requirements. As time progressed, the incentive to

[4] See Peter Hogg's letter to the Department of Finance, which was referenced by Elizabeth May in the House of Commons. http://elizabethmaymp.ca/wp-content/uploads/peter_hogg_fatca.pdf

over-report has gradually increased; Bill C-31 increases it further still. We would strongly urge the Committee to advise the government to proceed with caution to avoid the potential for scope creep.

III. Creation of the Administrative Tribunals Support Service of Canada

Finally, Bill C-31 includes a significant change for many federal administrative tribunals. As it stands now, most federal administrative tribunals qualify as "government institutions" and as such, are subject to the *Privacy Act*. Bill C-31 removes six tribunals[5] from the Schedule to the *Privacy Act*.

Creation of a central support service

This Bill creates a new body, the Administrative Tribunals Support Service of Canada (ATSSC), and tasks it as the sole provider of registry, administrative, research and analysis services for eleven administrative tribunals.[6] The ATSSC is also proposed to be made subject to the *Privacy Act*. It is not immediately evident what the implications are for individuals seeking a right of access to their personal information held by the tribunals which are no longer subject to the *Privacy Act*; as such, my officials sought clarification on this issue. It is our understanding that given the ATSCC is expected to be the custodian of all personal information for the tribunals which it supports, an individual's right of access to their personal information under the *Privacy Act* should be unimpeded. We will be interested to review any associated Regulations to ensure that this is, in fact, the case.

Open Court Principle and the Protection of Privacy

The open court principle seeks transparency in decision-making processes. However, the traditional scope of the open court principle was established at a time when access to the court or hearing room could be controlled. It is now a common practice for administrative tribunals to publish their reasons for decision on the Internet, potentially exposing complainants to publicity that was not contemplated decades ago. Given this new body may assume the responsibility for posting of decisions on administrative tribunals websites, the time has come for mandatory procedures to be developed regarding how federal tribunals can balance the open court principle with their responsibilities to protect personal information.

In 2010, we issued guidance[7] on this matter, which complements direction[8] issued in 2005 by the Canadian Judicial Council. Our guidance, which is non-binding, recommends that tribunals to strike an effective balance of the complainant's rights and the open court principle

---

[5] (1) Canada Industrial Relations Board, (2) Canadian Cultural Property Export Review Board, (3) Canadian Human Rights Tribunal, (4) Canadian International Trade Tribunal, (5) Registry of the Public Servants Disclosure Protection Tribunal and (6) the Specific Claims Tribunal.

[6] Specifically, (1) the Canada Industrial Relations Board; (2) the Canadian Cultural Property Export Review Board; (3) the Canadian Human Rights Tribunal; (4) the Competition Tribunal; (5) the Review Tribunal; (6) the Canadian International Trade Tribunal; (7) the Transportation Appeal Tribunal of Canada; (8) the Social Security Tribunal; (9) the Public Servants Disclosure Protection Tribunal; (10) the Specific Claims Tribunal; and (11) the Public Service Labour Relations Board.

[7] Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals available at http://www.priv.gc.ca/information/pub/gd_trib_201002_e.asp

[8] Use of Personal Information in Judgments and Recommended Protocol available at https://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_UseProtocol_2005_en.pdf

by limiting the amount of personal information that is released, either through redaction or by using a “web exclusion protocol” which essentially prevents search engines from “finding” and indexing the decision pages. However, it has come to our attention that there appears to be variation on how tribunals address this issue. The creation of a consolidated administrative support service is an opportunity to harmonize current practices. In this regard, we would strongly recommend that the Government issue formal, binding guidance on this issue to ensure that tribunals meet their privacy obligations.

Conclusion

In conclusion, I have touched on some of the privacy issues in this Bill which, I believe, are of concern for all Canadians. In terms of changes to the proceeds of crime regime as well as FATCA, in the absence of evidence to the contrary, this Bill appears to introduce privacy-invasive measures disproportionate to the identified threat. Should the Bill pass, we would stress that organizations that find themselves subject to the new measures introduced therein must be made aware, through education and outreach activities, of the limits of their reporting responsibilities. My Office will continue to provide guidance, particularly to the private sector, on how best to ensure that privacy rights are respected in this climate of ever-expanding encroachment into the private lives of Canadians. As for the creation of the Administrative Tribunals Support Service of Canada, the opportunity has come for guidance to be issued with respect to balancing the open court principle and protecting the privacy rights of those who appear before tribunals.

Thank you once again for the opportunity to present the Committee with our views on the proposal.

Sincerely,

Chantal Bernier
Interim Privacy Commissioner

cc: Christine Lafrance, Clerk