



October 29, 2004

Hon. Joyce Murray
Minister of Management Services
Legislative Buildings
Victoria BC V8W 9A4

Dear Minister:

Comments on *Freedom of Information and Protection of Privacy Amendment Act, 2004, S.B.C. 2004, c. 64 (Amending Act)*—OIPC File No. 21120

As promised in my October 8, 2004 letter to you, I write to comment on the Amending Act, which came into force on receiving Royal Assent on October 21.

As your October 7 remarks in the House confirm, the Amending Act is intended to address USA Patriot Act implications for the personal information of British Columbians as a result of the outsourcing of public body services to US linked service providers. As you are aware, my office has been assessing the USA Patriot Act and outsourcing in British Columbia and our report on the matter was released today. The report can be found on our website through http://www.oipc.bc.ca/sector_public/usa_patriot_act/patriot_act.htm.

The general direction taken by the Amending Act is consistent with our report, which recommended legislative, contractual and practical mitigating measures. This letter addresses the implementation of legislative mitigating measures in the Amending Act. Many of the comments are, therefore, necessarily oriented around technical-legal questions about which I am open to further discussion with the government as required.

A. SUMMARY OF COMMENTS ON THE AMENDING ACT

- The Amending Act is a positive step forward in addressing risk of disclosure of personal information under the USA Patriot Act. The government should, however, consider further amendments to the *Freedom of Information and Protection of Privacy Act* (FOIPPA) to address the issues raised below.
- In our report, we recommend that the government enact an express prohibition against disclosure of personal information in response to a foreign demand for disclosure, including a court order made under the US Foreign Intelligence

Surveillance Act (FISA) or a national security letter issued by the FBI under a variety of US statutes. The government is to be commended for having introduced changes along these lines, but it should consider clarifying and strengthening the new provisions as discussed below.

- Although I can see why the government might choose not to retrospectively prohibit location of personal information outside Canada—one of the new disclosure rules—there are good reasons for the new measures prohibiting disclosure of personal information (including personal information located in Canada) in response to a foreign demand for disclosure to apply to existing outsourcing contracts. The government should consider correcting this situation by amending FOIPPA so that the prohibition against disclosure in response to a foreign demand for disclosure applies to existing outsourcing contracts.

B. DISCUSSION

1. Summary of Report Conclusions

Before commenting on the Amending Act, let me summarize the most relevant conclusions in our report regarding privacy, the USA Patriot Act and FOIPPA¹:

- British Columbia residents can reasonably expect that their personal information located in British Columbia will be used and disclosed only in accordance with the law properly applicable in British Columbia.
- Outsourcing of public body functions to private contractors is not inconsistent with FOIPPA. A public body cannot, however, outsource functions in circumstances that would reduce security arrangements required by s. 30 of FOIPPA below those required of the public body directly:

The head of a public body must protect personal information in the custody or under the control of the public body by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

- The steps that public bodies must take to protect personal information in outsourcing arrangements depend on the meaning of s. 30, especially the words “reasonable” and “unauthorized”. In assessing the reasonableness of security arrangements, the nature of the personal information involved and the seriousness of the consequences of its unauthorized disclosure need to be taken into account. That said security arrangements to protect against unauthorized disclosure are necessary for all personal information, regardless of sensitivity.

¹ The discussion in this section relies on the wording of FOIPPA as of October 19, 2004.

- Any access, collection, use, disclosure or disposal of personal information that is authorized or required by or under foreign law, including US law, is “unauthorized” under s. 30 of FOIPPA because a foreign law is not a law properly applicable in British Columbia.
- Section 33 of FOIPPA spells out circumstances where public bodies may disclose personal information—for example, in accordance with treaties or to law enforcement agencies in certain cases—but none of the s. 33 circumstances apply to allow disclosure in direct response to court orders made in the US under FISA or in response to national security letters issued by the FBI under various US statutes.
- US courts have been willing over the years to order disclosure, for the purpose of US proceedings, of records held outside the US, as long as a person or corporation subject to the US court’s jurisdiction has control of those records, in the sense of a legal or practical ability to access them.
- Some US courts have found that control of records exists whenever a US parent-Canadian subsidiary corporate relationship exists, regardless of the contractual or practical arrangements between, for example, a British Columbia public body and the service provider or its US parent. Other US courts, however, have been influenced by contractual or practical arrangements regarding control.
- If the US Foreign Intelligence Surveillance Court (FIS Court) decides that a US located corporation has control over Canadian located records and thus is able to obtain the records and produce them in the US, there is a reasonable possibility that it could issue a FISA order compelling the US located corporation to produce records that are held in Canada and are under the US located corporation’s control.
- A ban on outsourcing is not a practical or effective response to this risk. The sensible solution is to put in place legislative, contractual and practical mitigating measures against illegal and surreptitious access.
- Some US courts have upheld subpoenas ordering corporations to disclose records located outside the US, even where foreign law prohibits disclosure of the records. Other US courts have been influenced not to order disclosure by the existence of a foreign law prohibiting it. The FIS Court might decline to order disclosure in the face of a clear and strong British Columbia statutory prohibition against disclosure and, in addition to implementing tailored contractual and practical arrangements when outsourcing, such a provision should be enacted.

Our report, therefore, calls for an express and direct legislated prohibition against disclosure in response to foreign court orders and for implementation of contractual and practical arrangements to address unauthorized disclosure or access. The

government is to be commended for having introduced a legislated prohibition in the Amending Act, and for its commitment that tailored contractual and practical arrangements will be implemented in outsourcing to address unauthorized disclosure and access.

The government's decision to legislatively preclude, expressly, the location of British Columbians' personal information outside Canada except under tightly controlled circumstances is also a significant step.

2. Comments on the Amending Act

As indicated above, and subject to the comments below, the Amending Act is a laudable piece of legislation.

a. *Transitional provisions*

My October 18 letter to you asked for further information to enable me to comment on the transition provisions found in s. 23 of the Amending Act. The speed with which the Amending Act has been brought into force effectively removes my concern that public bodies would have had too long a grace period during which they could enter into outsourcing contracts free of the new disclosure rules under the Amending Act.

Putting aside concern about the length of any grace period, a significant concern remains about the transition provisions. I can see why the government might choose not to retrospectively prohibit location of personal information outside Canada—one of the new disclosure rules—but why does the new prohibition against disclosure of personal information (including personal information located in Canada) in response to a foreign demand for disclosure not apply to existing outsourcing contracts?

The issue is that there may well be existing outsourcing contracts under which a US linked contractor has custody of personal information in Canada. It would not frustrate the contract or inappropriately burden the contractor if the new prohibition against disclosure in response to a foreign demand for disclosure—notably a US court order under FISA—were to apply in such a case. Because of the transition provisions in the Amending Act, however, the disclosure prohibition does not apply and personal information involved in such an outsourcing remains vulnerable to US access under FISA despite the government's stated intention to protect such information. This is not desirable.

Similarly, the new obligation under s. 30.2 of FOIPPA to report to you, as the minister responsible for FOIPPA, any foreign demand for disclosure does not, because of the Amending Act's transition provisions, apply to existing outsourcing contracts. This is not desirable.

The government should consider correcting this situation by further amending FOIPPA so that the new disclosure rules, other than the rule prohibiting location of personal information outside Canada, apply to already existing outsourcing contracts.

b. Prohibition against foreign disclosure

Recommendation 1 of our report calls on the government to enact a clear and strong legislative prohibition against disclosure of personal information located in Canada in response to a foreign demand for disclosure. The Amending Act has introduced measures along these lines, but the government should consider further amendments for the following reasons.

I will first describe my understanding of how the intended prohibition against disclosure introduced by the Amending Act works.

Section 31.1 provides that the requirements and restrictions of, among other aspects of Part 3 of FOIPPA, ss. 33.1 and 33.2 also apply to “employees, officers and directors” of public bodies. This covers service providers under outsourcing arrangements because the new FOIPPA definition of “employee” includes service providers. (The employees and associates of service providers are also subject to the new disclosure rules because s. 31.1(b) covers them.)

Section 30.4 provides that anyone described in s. 31.1 who has access to personal information—whether that access is authorized or unauthorized—must “not disclose that information except as authorized under this Act.” Section 74.1, a new provision, makes it an offence to contravene the s. 30.4 prohibition against unauthorized disclosure. Before s. 74.1 was introduced, unauthorized disclosure of personal information was not an offence²—it could only be the subject of a complaint to the Information and Privacy Commissioner.

Sections 33.1 and 33.2 of FOIPPA describe authorized public body disclosures of personal information. Section 33.1 regulates public body disclosures of personal information inside or outside Canada (further comments about s. 33.1 are found below) while s. 33.2 provides rules for disclosure inside Canada.

Section 33.1 does not list as an authorized disclosure of personal information any disclosure in response to a subpoena, warrant or court order. Section 33.2(b), by contrast, allows a public body to disclose personal information in Canada in response to a subpoena, warrant or court order issued by a court, person or body “in Canada” with jurisdiction to compel disclosure.

The former s. 33(e) authorized disclosure of personal information in response to a subpoena, warrant or court order but did not expressly state that the court or other body must be Canadian. As our report says, we consider that this limitation was implicit in s. 33(e). The new provision is much more explicit about disclosure in

² Section 5 of the *Offence Act* provides: “A person who contravenes an enactment by doing an act that it forbids, or omitting to do an act that it requires to be done, commits an offence against the enactment.” Section 74(3) of FOIPPA, however, provides that: “Section 5 of the *Offence Act* does not apply to this Act.” Section 74(1) and (2) prescribe specific offences under FOIPPA and section 74.1 of the Amended Act has now added contravention of the new section 30.4 to the list of offences under FOIPPA.

response to a foreign order being unauthorized than was the previous wording and the s. 74.1 offence provision is a significant addition.

It is not clear, however, why the new s. 30.2(1)(b) qualifies the definition of “foreign demand for disclosure” by requiring the foreign demand to be “for the unauthorized disclosure of personal information to which this Act applies”. Does this suggest that there could be a foreign court order or subpoena for disclosure of information to which FOIPPA applies that would *not* involve unauthorized disclosure? It is possible that a British Columbia law could specifically provide that a public body is authorized to disclose personal information in response to a foreign order, although I am not aware of such a provision off-hand. This would, however, in my view, make the disclosure a disclosure in accordance with a British Columbia enactment, not a foreign court order.

As discussed in our report, a US court, when considering whether to order disclosure of records from abroad, can be expected to consider and interpret a foreign legislative prohibition against disclosure. Although the Amending Act changes to FOIPPA create a prohibition, it does so in a manner that is, in my view, less direct than is desirable. I am not quibbling about legislative drafting when I suggest that a direct, forceful and unambiguous prohibition would be better.

Section 30.1, for example, clearly and directly requires that all personal information be stored and accessed in Canada. The prohibition against compliance with foreign disclosure demands should be just as direct. It should directly and expressly provide that “personal information in the custody or under the control of a public body must not be disclosed inside or outside Canada in response to a foreign demand for disclosure” (with the term “foreign demand for disclosure” being revised to clarify what is now s. 30.2(1)(b), discussed above).

c. Authorized disclosure inside or outside Canada

Subject to two exceptions, s. 30.1 of FOIPPA now allows personal information to be “stored only in Canada and accessed only in Canada”. Section 30.1(b) permits storage of personal information in another jurisdiction and access from another jurisdiction “for the purpose of disclosure allowed under this Act”. This requires analysis of the new s. 33.1 of FOIPPA.

Disclosure under enactments

Section 33.1(1)(c) provides that a public body can disclose personal information “in accordance with an enactment of British Columbia or Canada that authorizes or requires its disclosure”. This same language was in place before the Amending Act.

It would be better if s. 33.1(1)(c) were to provide that disclosure of personal information is permitted “outside Canada” only where an enactment “expressly” authorizes it. The present language invites argument, for example, that a general legislative authority or requirement to investigate a matter implicitly carries authority to disclose personal information outside Canada for investigative purposes.

I acknowledge that one could argue that, in the present context, the authority or requirement under an enactment would have to be quite specific to intend out of country disclosure. Still, I am concerned that, because s. 33.1(1)(c) does not clearly require express authority to permit out of country disclosure, controversies could arise about whether the new wording of s. 33.1(1)(c) protects against out of country disclosure. The government should consider amending the present language of s. 33.1(1)(c) to permit out of country disclosure only where expressly authorized or required by an enactment of British Columbia or Canada. This would also make the wording of s. 33.1(1)(c) in this regard consistent with the wording of s. 26(a), which requires “express” authorization for the collection of personal information.

Rules for information sharing

Section 33.1(1)(d) permits disclosure of personal information “in accordance with a treaty, arrangement or agreement” that “authorizes or requires its disclosure” and is “made under an enactment of British Columbia or Canada”. This is, again, the same language that existed before the Amending Act. Two particular comments arise out of this provision.

The first is similar to the above-identified comment that s. 33.1(1)(c) should be revised to allow disclosure of personal information outside Canada only with express authorization or requirement in an enactment. Here, the question is how specific or express the statutory authority should have to be to authorize information sharing. As it stands, s. 33.1(1)(d) refers in a very general manner to the making of an agreement or “arrangement” under an enactment. Again, in light of concern about access to personal information under FISA, FOIPPA should provide that a statutory authority or requirement for information sharing has to be explicit as to disclosure outside Canada. As s. 33.1(1)(d) stands, we have to infer that such specificity of authority is required and this opens the way for controversies as to legislative intention. This may require consequential amendments to other British Columbia statutes.

Second, I am concerned about the breadth of the information sharing authority found in s. 33.1(1)(d), especially because I am aware of no meaningful standards for information sharing or rules governing secondary use of personal information by recipient organizations. The issue is not merely what information sharing agreements are out there and what standards and conditions, if any, apply to the contents of those agreements, but also what enactments of British Columbia or Canada exist that in some general way (implicitly) authorize possibly indiscriminate and unrestricted sharing of personal information.

Our report expresses concern that there is incomplete information about the kinds of personal information being shared under information sharing agreements, the nature of information sharing and its extent. We also observe that the provincial government must substantially improve its compliance with s. 69 of FOIPPA, which requires disclosure of information sharing agreements by government ministries.

Recommendation 9 in our report is intended to address the lack of information about the nature and extent of information sharing:

The government of British Columbia should:

- (a) undertake a comprehensive and independent audit of interprovincial, national and transnational information sharing agreements affecting all public bodies in British Columbia;
- (b) use the audit to identify and describe operational and planned information sharing activities, including in each case: the kinds of personal information involved, the purposes for which it is shared, the authority for sharing it, the public bodies or private sector organizations involved, and the conditions in place to control the use and security of the information shared;
- (c) publicly release the audit report (including timely posting on a readily accessible government of British Columbia website);
- (d) act on deficiencies or other problems indicated by the audit;
- (e) conduct and publish periodic follow-up audits and reports to ensure ongoing transparency and accountability in this area; and
- (f) require information sharing agreements entered into by all public bodies to be generally available to the public (including timely consolidated posting on a readily accessible government of British Columbia website).

The audit contemplated by Recommendation 9 is, as noted in our report, an important step toward appropriate transparency, controls and oversight of information sharing. Once Recommendation 9 has been fulfilled, the government should consider amending FOIPPA to:

1. state that information sharing agreements are required to be in writing (s. 33.1(1)(d) and s. 33.1(2)(b) are inconsistent on this point),
2. eliminate information sharing under an “arrangement” in s. 33.1(1)(d) and s. 33.1(2)(b), which, it seems to me, arguably could include unwritten, casual measures that would not properly address the objectives of transparency and accountability identified in our report,
3. authorize information sharing agreements only where expressly authorized by an enactment (the government has, in the past few years, on several occasions acted on our advice to amend legislation to provide explicitly for information sharing agreements), and
4. ensure that information sharing agreements clearly identify restrictions on use of shared personal information by the recipient organization and prohibit any uses not explicitly provided for in those restrictions.

Ministerial consent to disclosure outside Canada

Section 33.1(3) allows the minister responsible for FOIPPA to, by order, allow disclosure of personal information outside Canada under any aspect of s. 33.2 “in specific cases or specified circumstances, subject to any restrictions or conditions that the minister considers advisable.” This appears to be intended to leave room to allow disclosure outside Canada in extraordinary circumstances.

If this is correct, the government should consider making s. 33.1(3) more clearly serve that aim by allowing ministerial disclosure outside Canada only where it is necessary and then only in accordance with specific and limited criteria that are established by regulation under FOIPPA.

Further, it is not clear, given the wording of s. 42(1)(a) and s. 42(2), that the Information and Privacy Commissioner can entertain a complaint under s. 42 about a ministerial order for disclosure under s. 33.1(3). This should be rectified. Such a role would be consistent with the Information and Privacy Commissioner’s role in providing independent oversight of decisions by ministers as the heads of public bodies under FOIPPA and conducting investigations to ensure compliance with any provision of FOIPPA.

d. Penalties for unauthorized disclosure

We discuss in our report how US courts can be expected, in deciding whether to order disclosure of records located outside the US, to consider a foreign prohibition against disclosure. They can also be expected to consider the penalties under foreign law for violating the foreign disclosure prohibition, in part in order to assess the importance to the foreign country of its prohibition against disclosure.

It is now an offence to disclose personal information without authority under FOIPPA and the Amending Act also creates other related offences. Section 74.1(5) provides for fines for corporations of up to \$500,000; up to \$25,000 for partnerships or individuals who are service providers; and up to \$2,000 for other individuals.

These fine thresholds are not as high as they should be to appropriately signal to US courts the seriousness of the public policy reflected in FOIPPA, including the foreign disclosure rules under Part 3 of FOIPPA. The maximum fines should also be higher to better reflect the potential severe prejudice of unauthorized disclosure and to more effectively deter such conduct. Terms of imprisonment should also be available as punishment.

There is plenty of precedent for higher maximum fines for serious provincial offences. Section 120 of the *Environmental Management Act*, SBC 2003, c. 53, for example, provides for a maximum fine of \$1,000,000 for various pollution-related offences. There should be no distinction in FOIPPA in the maximum fine as between corporations, individuals or partnerships that are service providers. The maximum fine for individuals who are not service providers should be higher than the Amending Act’s \$2,000–\$50,000 would be a more appropriate amount.

There is also precedent for terms of imprisonment for serious provincial offences. Section 155(2) of the *Securities Act*, RSBC 1996, c. 418, for example, provides, in the case of an individual, for a maximum fine of \$1,000,000 or up to 3 years imprisonment, or both. The addition of liability for imprisonment, in the alternative or in addition to a fine, would be highly desirable with respect to offences under FOIPPA.

The government should also consider clarifying the applicability to public bodies of the unauthorized disclosure prohibition in s. 30.4 and the related offence provision in s. 74.1(1). The wording of s. 30.4 and its incorporation of persons referred to in s. 31.1 is confusing on this point. In my view, these provisions should be unequivocally applicable to public bodies, not just to their employees, officers and directors.

e. *Enforcing orders of the Information and Privacy Commissioner*

In other respects, the Amending Act has increased the Information and Privacy Commissioner's oversight responsibilities and powers. I will not address here what impact this may have on my office's budget resources. I will note, however, that, although the Amending Act has expanded the order making power in s. 58(3)(e) to include service providers, there still is no mechanism in FOIPPA for the enforcement of orders that I make under s. 58. Interested parties may challenge my orders by applying for judicial review by the Supreme Court of British Columbia, but there is no mechanism for my orders to be filed in the Supreme Court for enforcement.

In my February 5, 2004 submission to the all-party Special Committee of the Legislative Assembly to Review FOIPPA, I raised this issue and asked the Special Committee to recommend changes in this respect to enable the filing of my orders in the Supreme Court and their enforcement through that process. The Special Committee made that recommendation.³

There are many precedents in British Columbia legislation for filing tribunal orders in the Supreme Court and giving them the same force and effect as an order of the Court (an example is s. 163 of the *Securities Act*, RSBC 1996, c. 418 and s. 79 of the *Securities Act*, SBC 2004, c. 43 (not yet in force)).

In addition, the government's recent initiative in enacting new statutory powers legislation for administrative tribunals clearly contemplates the filing of tribunal orders in the Supreme Court for enforcement purposes (see s. 54 of the *Administrative Tribunals Act*, SBC 2004, c. 45). The extension of the principles of the new

³ Legislative Assembly of the Province of British Columbia, Report of the Special Committee to Review the *Freedom of Information and Protection of Privacy Act, Enhancing the Province's Public Sector Access and Privacy Law* (Fifth Session, Thirty-Seventh Parliament, May 2004), Recommendation 24: "Amend the Act to provide a mechanism for the enforcement of the Commissioner's orders as orders of the Supreme Court of British Columbia."

Administrative Tribunals Act to the enforcement procedures under FOIPPA would be very beneficial indeed.

The government's commitment to have the best access and privacy law in Canada, reflected in its enactment of the Amending Act, should encompass further amendments to FOIPPA to improve my office's ability to monitor and enforce FOIPPA compliance. There is no doubt in my mind that improvements to our enforcement powers are indispensable to the effectiveness of the Amending Act amendments.

f. The best access and privacy legislation

The government's commitment to having the best access and privacy legislation in Canada is a commitment I support whole-heartedly. The government moved with speed in passing the Amending Act to address concerns about the privacy implications of the USA Patriot Act in relation to the outsourcing of public services in British Columbia.

In my view, British Columbians would also be well served by the enactment of the improvements that were recommended unanimously by the Legislative Assembly Special Committee to Review FOIPPA in its report of May 2004. These improvements are good public policy and many are long overdue.

I urge the government to act on the recommendations I have made today with respect to the USA Patriot Act and to take immediate steps to implement the work of the Special Committee. Implementation of these additional measures will complement and strengthen the provisions in the Amending Act and give British Columbia strong, modern and effective access and privacy legislation.

I should note that, in light of the public nature of the process leading to our USA Patriot Act report released today, this letter will also be made available publicly.

Yours sincerely,

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

cc: Hon. Geoff Plant, Attorney General
Carole James, Leader of the New Democratic Party
Joy MacPhail, Opposition House Leader
Cairine MacDonald, Deputy Minister, Management Services
Allan Seckel, Deputy Attorney General