SUBMISSIONS OF THE CANADIAN BAR ASSOCIATION (BRITISH COLUMBIA BRANCH)

TO THE

LEGISLATIVE ASSEMBLY OF BRITISH COLUMBIA

SPECIAL COMMITTEE

TO REVIEW THE

PERSONAL INFORMATION PROTECTION ACT

Issued By:

Canadian Bar Association
British Columbia Branch

Special Committee of the
Freedom of Information and
Privacy Law Section

September 2014

TABLE OF CONTENTS

SECTION	PAGE
PREFACE	3
EXECUTIVE SUMMARY	6
SUBMISSIONS	7
Introduction	7
Warrantless Disclosure	8
Mandatory Privacy Breach Notification	12
The Section's February 12, 2008 Submissions	12
2009 Amendments to the Alberta *Personal Information Protection Act*	13
Contemplated Amendments to the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)	15
Constitutional Implications of *Alberta V. UFCW*	21
Resourcing The OIPC	26
CONCLUSION	28

\

PREFACE

Formed in 1896, the purpose of the Canadian Bar Association (British Columbia Branch) (the "CBABC") is to:

- enhance the professional and commercial interests of our members;
- provide personal and professional development and support for our members;
- protect the independence of the judiciary and the Bar;
- promote access to justice;
- promote fair justice systems and practical and effective law reform; and
- promote equality in the legal profession and eliminate discrimination.

The CBA nationally represents approximately 39,000 members and the British Columbia Branch itself has over 6,900 members. Our members practice law in many different areas. The CBABC has established 78 different sections to provide a focus for lawyers who practice in similar areas to participate in continuing legal education, research and law reform. The CBABC has also established standing committees and special committees from time to time.

The Freedom of Information and Privacy Law Section (the "Section") of the CBABC is pleased to respond to the call for submissions of the Legislative Assembly of British

Columbia Special Committee ("Special Committee") to review the *Personal Information Protection Act,* R.S.B.C. 2003, c. 63 ("*PIPA*").[1]

The Section is comprised of members of the CBABC who share an interest, and/or practise law in areas that pertain to access of information and privacy law. As our membership represents a vast range of perspectives, interests and practices, it is difficult for the Section to make submissions to the Special Committee that would reflect the views of all members. Accordingly, rather than attempting to reconcile disparate points of view, the Section Executive decided to solicit and record input from individual members in its submissions to the Special Committee. As a result, the Section's submissions do not necessarily adopt a unified position on a particular issue. The following submissions reflect the views of individual Section members, and not necessarily the views of the CBABC or the Section as a whole. We are grateful for the work of Sinziana Gutiu and Fiona McFarlane in preparing these submissions.

This is the second occasion that a Special Committee has reviewed *PIPA*, and the second occasion that the Section has made submissions to the Special Committee. The Section's previous submissions dated February 12, 2008 (the "2008 Submissions"), suggested changes regarding mandatory breach reporting, public interest discretion, settlement and confidential discussions, business transactions, cross-border data flows, and publicly available information.[2] The Special Committee's Report dated April 2008

[1] A copy of the legislation can be found at http://www.bclaws.ca/civix/document/id/complete/statreg/03063_01.
[2] The 2008 Submissions are available online at http://cbabc.org/CMSPages/GetFile.aspx?guid=c1e92dee-102d-4a93-af59-a88daf60ed32.

adopted a number of the Section's suggested changes, including those related to mandatory breach notification.

The Section's present submissions to the Special Committee continue to suggest changes to mandatory breach reporting, and also include new suggestions, related to warrantless disclosure, constitutional considerations arising out of the Supreme Court of Canada's decision in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 SCR 733 ("*Alberta v. UFCW*")[3] and providing resources to the Office of the Information and Privacy Commissioner for British Columbia ("OIPC").

[3] The decision can be found on the Supreme Court of Canada website (http://scc-csc.lexum.com) or at http://www.canlii.org/en/ca/scc/doc/2013/2013scc62/2013scc62.html.

EXECUTIVE SUMMARY

The Section's submissions, although not representative of the CBABC or of the view of all Section members, reflect the common goal of improving the interpretation and application of *PIPA*.

In the six years since the 2008 Submissions to the Special Committee, the depth and volume of personal information possessed by private organizations has increased, and the methods of collection and dissemination of personal information by the private sector have become more sophisticated as a result of technological innovations. Section 2 of *PIPA* requires an appropriate balancing of private sector needs with individuals' rights to protect their personal information. As such, it is to the benefit of both individuals and private organizations to ensure that *PIPA's* objectives respond to the ever-changing landscape of the collection, retention and exchange of personal information.

The Section members' proposed suggestions reflect a variety of legal perspectives. Overall, members' responses suggest that *PIPA* is working well in practice, and that minor changes are likely sufficient to strengthen the balance between the two-fold purposes of the Act.

SUBMISSIONS

The Section members submit suggestions on the following topics:

- warrantless disclosure;
- mandatory privacy breach notification;
- constitutional implications of *Alberta V. UFCW*[4]*;* and
- resourcing the Office of the Information and Privacy Commissioner for BC.

Introduction

Privacy is essential to a free and democratic society and has long been recognized in Canada as a fundamental value. The Supreme Court of Canada recently commented that "[t]he importance of the protection of privacy in a vibrant democracy cannot be overstated […] democracy depends on an autonomous, self-actualized citizenry that is free to formulate and express unconventional views. If invasions of privacy inhibit individuality and produce conformity, democracy itself suffers." [5] Indeed, it is because they protect and support our fundamental democratic values that privacy laws are now considered to be quasi-constitutional:

> The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional"

[4] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401* 2013 SCC 62 (CanLII). In this case, the Alberta *Personal Information and Protection Act* S.A. 2003, c. P-6.5 (the "*Alberta PIPA*"), which is almost identical to the British Columbia *PIPA*, was considered by the Supreme Court of Canada

[5] *Supra*, para. 22.

> because of the fundamental role privacy plays in the preservation of a free and democratic society.[6] [emphasis added]

And with every new technological leap forward, the public's concern with privacy rights, risks and protections grows ever more pronounced. Today, when new technologies give organizations "an almost unlimited capacity to collect personal information, analyze it, use it and communicate it to others for their own purposes,"[7] the objectives of laws protecting privacy are of a greater significance than ever.

Warrantless Disclosure

In the spring of this year, the Supreme Court of Canada decided *R. v. Spencer* ("*Spencer*"),[8] in which it said that a general provision in a law that permits an organization to disclose information to law enforcement does not mean that the police can get personal information without a warrant. In other words, organizations can't just hand over information to law enforcement agencies upon request.

The Court in *Spencer* also explained that the concept of "privacy" in relation to information is very broad, including notions of confidentiality and secrecy, but also involving control. This inclusion of control "derives from the assumption that all

---

[6] *Supra*, at para 9. In support of this principle, the Court cited *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53 (CanLII), [2002] 2 S.C.R. 773, at para. 24; *Dagg v. Canada (Minister of Finance)*, 1997 CanLII 358 (SCC), [1997] 2 S.C.R. 403, at paras. 65-66; *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, 2006 SCC 13 (CanLII), [2006] 1 S.C.R. 441, at para. 28.

[7] *Supra*, para. 20.

[8] *R. v Spencer*, 2014 SCC 43 (CanLII) available on the Supreme Court of Canada website (http://scc-csc.lexum.com) or at (http://www.canlii.org/en/ca/scc/doc/2014/2014scc43/2014scc43.html).

information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit".[9]

Therefore, the Court concluded that even in circumstances where information will be communicated and cannot be thought of as secret or confidential, "situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected."[10] [emphasis added]

However, control, confidentiality and secrecy aren't the only important values embedded in the concept of "privacy." Anonymity has been increasingly recognized as one element of privacy that is important in a free and democratic society. The Court said that anonymity permits individuals to act in public places while preserving their individual right to be free from identification and surveillance:

> In a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the 'situational landscape'"… The mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that as a practical matter, such a person

[9] Para. 40.
[10] *Ibid.*

> may not be able to control who observes him or her in public. Thus, in order to uphold the protection of privacy rights in some contexts, we must recognize anonymity as one conception of privacy.[11] [emphasis added]

Privacy regulation in the private sector is similarly informed by the protection of individual autonomy, control and anonymity.

Section 18(1)(j) of *PIPA* permits an organization to disclose personal information without consent if:

> the disclosure is to a public body or a law enforcement agency in Canada, concerning an offence under the laws of Canada or a province, to assist in an investigation, or in the making of a decision to undertake an investigation,
>
> (i) to determine whether the offence has taken place, or
> (ii) to prepare for the laying of a charge or the prosecution of the offence.

This section is confusing and overbroad because it appears to authorize disclosure of personal information to law enforcement without a warrant or production order, even where the individual has a reasonable expectation of privacy (and thus would be protected from an unreasonable search by section 8 of the Canadian Charter *of Rights*

[11] Para. 44.

and Freedoms (the "*Charter*")). In *R v. Spencer*, a similar provision in the federal *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*") was found by the Supreme Court of Canada not to authorize disclosure of personal information to police absent a warrant. We would suggest reviewing this provision to meet the standards enunciated by the Supreme Court of Canada in *R v. Spencer*, and to clarify that *PIPA* (like *PIPEDA*) does not grant any new authority to police in circumstances where they would otherwise require lawful authority.

While some Section members agree that section 18(1)(j) needs clarification regarding whether lawful authority is required, and what the nature of such authority would be prior to disclosure without consent, they caution that by proposing specific wording for an amendment, certain nuances required for legitimate police work may be compromised. As such, a number of Section members propose that any amendments to section 18(1)(j) requiring lawful authority before an organization can disclose personal information without consent, should not interfere with legitimate police work or with administrative or regulatory investigations, or take away an organization's ability to report a crime or provide information to prevent imminent harm to the health or safety of an individual.

Mandatory Privacy Breach Notification

The Section's February 12, 2008 Submissions

In its 2008 Submissions to the Special Committee, the Section advanced the varying views of its members with respect to the issue of mandatory breach notification.

While members' views varied regarding the necessity of introducing a mandatory requirement, there was general consensus that if such a requirement were to be introduced, careful consideration would need to be given to the following:

- **Threshold requirements** - articulating a clear threshold requirement for reporting to the Office of the Information and Privacy Commissioner; for example, the number of individuals affected, categories of information lost, recipient of the notification and timelines for and methods of effecting notification; and

- **Consistency** - ensuring that the substance of the threshold requirements is essentially the same under *PIPA*, *PIPEDA*, and the *Alberta PIPA*.

The Special Committee recommended in its April 2008 report that *PIPA* should include a provision expressly requiring organizations to notify affected individuals of certain

privacy breaches related to unauthorized disclosure and use of sensitive financial or health information.[12] To date, this recommendation has not been implemented.

In the time since the April 2008 Special Committee report was issued, other jurisdictions in Canada have taken positive steps to legislate mandatory breach notification.

2009 Amendments to the Alberta *Personal Information Protection Act*

Following the recommendation of its own Select Special Committee, Alberta amended the *Alberta PIPA* in 2009 to include a mandatory breach notification requirement. Alberta's next review of *PIPA* is scheduled to begin on July 1st, 2015.

The reporting requirement, as set out in section 34.1 of the *Alberta PIPA*, requires an organization to provide notice, without unreasonable delay, to the Alberta Privacy Commissioner of any incident involving the loss of or unauthorized access to, or disclosure of, personal information that was under the organization's control where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure. The notice to the Alberta Privacy Commissioner must conform to the information requirements of section 19 of the Personal Information Protection Act Regulation ("*Alberta PIPA Regulation")*.[13]

[12] Pages 7-8 of the Report which can be found online at http://www.leg.bc.ca/cmt/38thparl/session-4/pipa/reports/PDF/Rpt-PIPA-38-4-2008-APR-17.pdf.
[13] Alta. Reg. 366/2003 is available online at http://www.qp.alberta.ca/1266.cfm?page=2003_366.cfm&leg_type=Regs&isbncln=9780779749003 or http://www.canlii.org/en/ab/laws/regu/alta-reg-366-2003/latest/alta-reg-366-2003.html.

The notification requirement, as set out in section 37.1 of the *Alberta PIPA*, provides that the Commissioner may require a reporting organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure, in accordance with the information requirements set out in section 19.1 of the *Alberta PIPA Regulation*, and within the timeline imposed by the Commissioner. The Commissioner also has the power to impose additional terms and conditions on the organization in connection with the notification as the Commissioner deems appropriate, as provided in section 37.1(2) of the *Alberta PIPA*.

Additional relevant provisions in the *Alberta PIPA* include:

- **Voluntary notification** - Section 37.1(7) provides that nothing in the mandatory breach notification requirement prevents an organization from notifying individuals voluntarily, of its own accord.

- **Failure to notify is an offence** - Section 59(1)(e.1) provides that it is an offence under the *Alberta PIPA* to fail to notify the Commissioner when required by section 34.1. The penalty for committing an offence is a fine of not more than $10,000 for individuals, and $100,000 for persons other than individuals.[14] Neither an organization nor an individual may be found guilty of an offence if they

[14] See s. 59(2) of the *Alberta PIPA*.

can demonstrate to the satisfaction of the court that they acted reasonably in the circumstances that gave rise to the offence.[15]

Contemplated Amendments to the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)

More recently, Bill S-4 ("*Digital Privacy Act"*), which was passed by the Senate of Canada on June 16, 2014, sets out to amend *PIPEDA*, including the introduction of a mandatory breach notification requirement.[16] The new sections 10.1, 10.2 and 10.3 of *PIPEDA*, dealing with "breaches of security safeguards", would require the following:[17]

- **Notification to the Privacy Commissioner of Canada** where an organization has experienced a breach of security safeguards and it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual;

- **Notification to individuals** whose personal information is involved if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual; and

[15] See s. 59(4) of the *Alberta PIPA*.
[16] Bill S-4 is available online at http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6670555.
[17] Bill S-4 also provides that specifics of the reporting requirements would be set out in regulations.

- **Notification to other organizations and/or government institutions** if the notifying organization believes that the other organization(s) or government institution(s) may be able to reduce the risk of harm that could result from the data breach or mitigate that harm.

In addition, “significant harm” is defined to include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

The factors relevant to determining whether a “real risk” of significant harm exists include the sensitivity of the personal information involved in the breach, the probability that the personal information has been or is being or will be misused, and any other factor that is prescribed by regulation.

The CBA at the National level made a formal submission in June 2014, to the Standing Senate Committee on Transport and Communications regarding Bill S-4. In that submission, the National CBA:

- draws the Committee’s attention to the need and desire to avoid the U.S. experience with breach notification, where a multitude of approaches adopted in various state and federal laws have created and imposed on organizations a confusing, inconsistent patchwork of obligations;

- reconfirms its previous advocacy for a balanced approach to mandatory breach notification that requires breach notification to individuals in some circumstances and reporting to the Commissioner in other, slightly narrower circumstances;

- generally supports the approach adopted in Bill S-4 as having taken account of issues raised in previous CBA submissions, specifically that:

    - the requirement is consistent with the general framework of *PIPEDA*;

    - the requirement is flexible in its application while allowing for greater specificity to be detailed in regulation; and

    - the requirement would create an exception to the informed consent requirement to enable organizations to notify certain third party organizations or government institutions in certain circumstances where there has been a breach.[18]

The National CBA's submission also made the following recommendations for improvement to the effectiveness of the breach notification regime:

[18] The submission of the National CBA is available at https://www.cba.org/cba/submissions/pdf/14-34-eng.pdf, while the proceedings of the Standing Senate Committee on Transport and Communications, Issue 7, Evidence, June 3, 2014, including the evidence of Jean Nelson of the CBA, is available at http://www.parl.gc.ca/Content/SEN/Committee/412/trcm/07ev-51484-e.htm?Language=E&Parl=41&Ses=2&comm_id=19.

- different threshold criteria should be established for notifying individuals versus reporting to the Commissioner, with such criteria reflecting the differing objectives of the two obligations (consistent with previous submissions of Bill S-4's predecessors, Bills C-12 and C-29, both of which died in prorogation); and

- failure to notify should not constitute an offence under *PIPEDA*, or attract a penalty (which recourse tends to be reserved for acts of malfeasance), but should be treated similar to other acts of non-compliance and be subject to the general *PIPEDA* complaint regime and available remedies, including the ability of the Federal Court to order payment of damages and/or for an organization to change its information practices.[19]

While there are still members of the Section that continue to question the need for the introduction of a mandatory breach notification requirement, given the legislative activity elsewhere in Canada, there is a sense of inevitability that it will be introduced in British Columbia.

In particular, if Bill S-4 becomes law and amends *PIPEDA*, it is an open question whether *PIPA* would be able to maintain its designation as legislation that is "substantially similar" to *PIPEDA* in the absence of a comparable requirement. The concept of "substantially similar" is discussed below.

[19] See pages 24-25 of the National CBA submission regarding Bill S-4 – *Digital Privacy Act* available at http://www.cba.org/CBA/submissions/pdf/14-34-eng.pdf.

To the extent that mandatory breach notification will become a reality for organizations subject to *PIPA*, the Section's members would like to reiterate and re-emphasize the need to achieve consistency, to the extent reasonably possible, with other breach notification regimes in Canada. However, Section members urge the Special Committee, in deliberating and recommending reporting and notification thresholds, to give careful consideration to the objectives served by reporting to the OIPC. In particular, whether the objectives for reporting should include:

- assisting the Commissioner in tracking the number, magnitude and type of breaches;

- giving the OIPC an opportunity to determine whether and how individual notification should occur;

- taking corrective action with respect to breaching organizations; or

- all of the above.

Section members also urge consideration regarding the objectives of notification of individuals, such as whether such objectives should include:

- allowing the individual the opportunity to mitigate potential harm;

- recognizing the individual's right to have knowledge of the management and disposition of his or her personal information and make informed choices about the organizations the individual does business with; or

- all of the above.

Additional considerations include whether a single threshold for both reporting and individual notification best serves the aforementioned objectives, or whether different thresholds for reporting versus notification are more appropriate.

Further, Section members ask the Special Committee to consider whether a failure to report or notify necessarily rises to the level of malfeasance inherent in the other acts and omissions that are currently designated as offences under section 56 of *PIPA*, or whether such a failure can adequately be addressed by the existing complaints process in *PIPA*.

Section members agree that the Special Committee should deliberate on the role that mandatory breach reporting will serve, and ensure that BC's reporting regime is consistent, to the extent reasonably possible, with other breach notification regimes in Canada.

Constitutional Implications of *Alberta v. UFCW*

The Information and Privacy Commissioner, in her briefing dated May 28, 2014 to the Special Committee, drew the Special Committee's attention the Supreme Court of Canada's decision in *Alberta v. UFCW*, where the Supreme Court of Canada concluded that the *Alberta PIPA* was unconstitutional because it limited freedom of expression. Specifically, the *Alberta PIPA* restricted a union's ability to collect, use or disclose personal information under specific circumstances.

In *Alberta v. UFCW*, the union video-taped and photographed the picket line near the main entrance of a casino at the West Edmonton Mall. The union had posted signs in the picketing area informing people that images of persons crossing the picket line might be placed on a website.

Several individuals, including employees and officers of the employer as well as members of the public, complained to the Office of the Information and Privacy Commissioner of Alberta (the "Alberta OIPC") that the recording of their images had been collected, used and/or disclosed contrary to the *Alberta PIPA*. As a result, the Alberta OIPC conducted an investigation.

This investigation revealed that none of the images were placed on a website, two pictures of the Vice-President of the casino were used on a poster displayed at the picket line, and images of his head were used in strike leaflets with captions intended to be humourous. The Alberta OIPC concluded that the union's activities were common

practice for both employers and unions during lawful strikes, and that the purpose of collection and use of the images by the union was, *inter alia*, to inform its members and the general public about relevant issues, provide a deterrent to violence on the picket line, and to preserve potential evidence if an investigation or legal proceeding was commenced.

Based on these findings, the Commissioner ruled that the collection, use and disclosure of personal information was for expressive purposes and concluded that the *Alberta PIPA* did not authorize collection, use and disclosure for expressive purposes meaning the union was found to be in violation of the *Alberta PIPA*.

Not able to challenge the constitutionality of the *Alberta PIPA* at the investigation stage, the union appealed the Commissioner's decision and argued that the *Alberta PIPA* infringed section 2 of the *Charter*, which states that:

> 2. Everyone has the following fundamental freedoms:
>
> …
>
> (*b*) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;

The Alberta Court of Queen's Bench and the Alberta Court of Appeal both concluded that the *Alberta PIPA* infringed the *Charter* and that the infringement was not justified but applied a different analysis in reaching the same conclusion.

At the Supreme Court of Canada, the nature of freedom of expression and expressive activity was reviewed in order to determine if the *Alberta PIPA* limited the union's freedom of expression. The Supreme Court of Canada also considered how the *Alberta PIPA* is substantially similar to *PIPEDA* because section 26(2)(b) of *PIPEDA* requires provincial privacy laws that apply to the private sector to be "substantially similar" in order to supplant the federal law.

The Supreme Court of Canada found that to the extent that the *Alberta PIPA* restricted the union's collection, use and disclosure of personal information for legitimate labour relations purposes, it violated the right to freedom of expression in section 2(b) of the *Charter*. In concluding that the *Alberta PIPA* "imposes restrictions on a union's ability to communicate and persuade the public of its cause, impairing its ability to use of its most effective bargaining strategies in the course of a lawful strike", the Supreme Court of Canada found that the restrictions were disproportionate to the *Alberta PIPA*'s objectives of providing individuals control over their private information.[20]

At the writing of these submissions, the *Alberta PIPA* has been declared invalid but that declaration has been suspended for 12 months (until November 2014), to allow the Alberta Legislature to review the *Alberta PIPA* and re-write and/or amend it to ensure its constitutionality.

[20] Paras, 37, 39 to 41.

In response to this ruling, the Alberta government and the Alberta OIPC have recommended a narrow amendment to the *Alberta PIPA*. The Alberta OIPC recommended that authorizing provisions be added allowing the collection, use or disclosure of personal information by unions for expressive purposes without consent, in the context of picketing during a lawful strike.[21]

The Special Committee must be cognizant of the on-going review in Alberta because provincial laws must be "substantially similar" to *PIPEDA* and should also be "substantially similar" to one another to minimize and eliminate a patchwork of privacy rules for the private sector. The current privacy law regime in Canada would be seriously undermined if organizations operating in multiple jurisdictions in Canada had to contend with different rules for the use, collection and disclosure of the private personal information of its customers, clients, employees, directors and contractors amongst others. In addition to introducing additional cost and complexity for the organizations, it would leave individuals in some jurisdictions vulnerable to misuse of their personal information.

The Information and Privacy Commissioner in her briefing to, and oral evidence before, the Special Committee advised that a narrow amendment to the *Alberta PIPA* has been proposed, and recommended that a similar amendment be adopted in BC.

[21] Letter to Honourable Jonathan Denis, Minister of Justice and Solicitor General and Honourable Doug Griffiths, Minister of Service Alberta, December 20, 2013, page 3 (http://www.oipc.ab.ca/Content_Files/Files/News/Denis_Griffiths_2013_PIPA_Website.pdf).

Members of the Section have suggested that maintaining *PIPA's* substantially similar status is a key consideration in the attempt to strike an acceptable balance between the constitutional right to freedom of expression, and the quasi-constitutional right to privacy.

One Section member suggested that the Special Committee may want to consider broadening the definition of "open to the public" or "available to the public" in sections 12(d) and (e), 15(d) and (e) and 18(d) and (e) to include information that is considered to be in the public domain to better align with circumstances where there would be no reasonable expectation of privacy. However, other Section members argue against broadening such terms, because in their view, defining what is open or available to the public is increasingly challenging in an era when in seconds, through social media, individual's personal information can be published and re-published without her or his knowledge or consent. Moreover, some Section members suggest that broadening the definition of these terms or otherwise expanding the notion of permitted collection without consent of "publicly available" information would undermine the protection of anonymity which is an important component of the right to privacy, and is discussed above at page 10 of these Submissions.

Some Section members view the plain meaning and sources prescribed by regulation as already contemplating a reasonable amount of information as being open or available to the public. Should the government identify other reasonable public sources for personal information which may emerge as society and technology evolves, the regulation can be amended.

In sum, Section members conclude that if a decision is made to amend the *PIPA* to more clearly align with the *Alberta v. UFCW* decision, the Special Committee must be cognizant of the need to maintain the legislation's substantially similar status; of the risks posed by an overbroad amendment; of the narrow issue before the Court in that case and the balancing that is inherent in all constitutional decision-making.

Resourcing the OIPC

The Office of the Information and Privacy Commissioner for BC provides essential guidance to legislators and the public on privacy rights and obligations; it is the key resource in the province for citizens and organizations seeking redress for contraventions of the law; and it provides substantial legal and policy analysis in respect of emerging issues of importance in respect of privacy, the intersection of privacy and technology and individual rights in British Columbia. The work of the OIPC is important not only because it is a regulator and as such a guardian of individual civil rights, but also because it contributes to the larger discussion related to use and development of technology, which is important for organizations to understand when making operational commitments. It does this work in an increasingly complex local, national and international environment.

While public awareness of and concern about privacy rights and obligations has increased, Section members have noted that this appears to be leading to increasing delay at in the investigation and adjudication of inquiries and complaints by the OIPC.

These delays can have negative consequences for complainants, and may allow privacy breaches to continue with impunity. Lengthy investigations due to lack of resources also impact private organizations that are the subject of the investigation or review, as the organizations incur increasing costs and uncertainty, and potential damage to their business relationships, such as if the complainant is a client or an employee of that organization. It is in the interest of both individuals and private organizations that the OIPC be provided with sufficient resources to complete matters as efficiently as possible.

Section members suggest that the Special Committee consider allocating additional full-time equivalents to the OIPC to ensure prompt and efficient investigation of privacy complaints in BC.

CONCLUSION

We would be pleased to discuss our submissions further with the Special Committee, either in person or in writing, in order to provide any clarification or additional information that may be of assistance to the Special Committee as it undertakes this legislative review.

Communications in this regard can be directed to:

RYAN BERGER

Co-Chair, CBABC Freedom of Information and Privacy Section

Bull, Houser & Tupper

Tel: 604-641-4956

Email: rpb@bht.com

SARA ANN LEVINE

Co-Chair, CBABC Freedom of Information and Privacy Law Section

Alliance Lex Law Corporation

Tel: 604-877-1057

Email: slevine@alliancelex.com