4 Alberta *PIPA*, SA 2003, c. P-6.5 as amended.
5 The structure and objectives of the B.C. *PIPA* are also very similar and may provide guidance as to risks and obligations.
6 See *United Food and Commercial Workers, Local 401 v. Alberta (Attorney General),* [2012] A.J. No. 427, 2012 ABCA 130 at para. 77 (appeal at the Supreme Court was heard on June 11, 2013); *Leon's Furniture Ltd. v Alberta (Information and Privacy Commissioner)*, [2011] A.J. No. 338, 2011 ABCA 94 at paras. 46–65.
7 *PIPITPA*, *supra* note 1, s. 7(1).
8 *Ibid.,* s. 8(4).
9 *Ibid.,* s. 7(2).
10 2009 Alberta *PIPA*, *supra* note 3, s. 22.
11 B.C. *PIPA*, S.B.C. 2003, c. 63, s. 20.
12 *Supra* note 1, s. 22(1).
13 *Ibid.,* s. 22(3).
14 *Ibid.*, s. 15(1).
15 *Ibid*., s. 15(3).
16 *Ibid.,* s. 5(2).
17 *Ibid*., s. 24(2).
18 *Ibid.*, ss. 24(4) and 25(2).
19 *Ibid.,* s. 33.
20 *Ibid*., s. 34.
21 Alberta *PIPA*, *supra* note 4, s. 34(1).
22 *Ibid.*, s. 34.1(1).
23 *PIPITPA*, *supra* note 1, s. 34(4).
24 *Ibid.*, s. 35.
25 C.C.S.M. c. F175.
26 C.C.S.M. c. P33.5.

Blurring of Personal and Professional E-mail Accounts

Timothy M. Banks
National Lead for the Privacy and Security Practice
Dentons Canada LLP

Not uncommonly, employees may forward information back and forth between personal and professional e-mail accounts. The reasons for this practice vary. Sometimes it is so that the employee can work on a matter while travelling. In these cases, the employee sometimes faces a real or simply perceived systems limitation. For example, the employee may not have remote access, the remote access authentication procedure may be perceived to be cumbersome, or certain functions (such as printing) may not be available. However, a more nefarious purpose may potentially exist for moving information back and forth between personal and professional e-mail accounts, such as the misuse or misappropriation of confidential information.

Recently, Elizabeth Denham, British Columbia Information and Privacy Commissioner (IPC), examined this issue in the context of an investigation into whether personal information was shared between the British Columbia government and the British Columbia Liberal Party in contravention of public sector privacy legislation.[1] It is important to note that no evidence of inappropriate sharing was found.[2]

However, the IPC raised concerns over the exchange of government information across work and personal e-mail accounts. In particular, the IPC was concerned that the use of personal e-mail accounts might involve improper disclosure of personal information contrary to the B.C. *Freedom of Information and Protection of Privacy Act* [*FIPPA*].[3] In particular, the storage of e-mail (containing personal information of British Columbians) outside Canada could violate s. 30.1 of the *FIPPA* that provides:

> A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:
>
> (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;
>
> (b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;
>
> (c) if it was disclosed under section 33.1 (1) (i.1) [certain disclosures relating to payments].

In addition, the use of e-mail providers that mine the content of the e-mail for the purposes of providing targeted advertising could involve a disclosure

outside Canada in violation of s. 33.1 of the *FIPPA*. This section prohibits disclosing personal information outside Canada unless one of the exceptions in that provision applies.

The IPC made a number of recommendations for change:

- Provide training on the use of personal e-mail accounts for government business, including ensuring compliance with the *FIPPA*'s restrictions on storing or disclosing personal information outside Canada.
- Ensure that all records relating to government business are located in government-controlled information management systems.
- Provide employees with sufficient technological resources to ensure that they do not have a reason to use personal e-mail in the course of government business.
- Ensure that government employees have mandatory privacy training on the separation of government roles from roles they may have in a political party.
- The BC Liberal Party should ensure that employees and volunteers have similar training regarding separation of roles.[4]

The issue of sharing between personal and professional e-mail accounts is particularly acute in the public sector where such sharing may have the effect (however inadvertently) of undermining record-keeping obligations and the public's rights to access government information. However, the issue should be of equal concern in the private sector where such sharing has the potential to subvert information security policies, data retention programs, and access to personal information requests under privacy legislation and to complicate the process of collecting and preserving documents in litigation.

---

1 *Investigation Report F13-04, Sharing of Personal Information as Part of the Draft Multicultural Strategic Outreach Plan: Government of British Columbia and the BC Liberal Party*, [2013] B.C.I.P.C.D. No. 21 [*Investigation Report*].

2 *Ibid*. at p. 3.

3 *FIPPA*, R.S.B.C. 1996, c. 165.

4 *Investigation Report*, *supra* note 1 at p. 25.