THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT AND THE CROSS-BORDER TRANSFER OF EMPLOYEE DATA

*By Candice Teitlebaum**

In May 2008, I discussed the impact of transborder data flows and the existence of the USA PATRIOT Act[1] in the context of personal health information. The disclosure of the personal information of Canadians outside of Canada elicits significant privacy concerns regardless of the type of personal information that is transferred. Accordingly, many of the recommendations regarding the cross-border transfer of personal health information remain applicable in the employment context.

It is increasingly common for large businesses to store records in off-site locations due to issues of space, and to avoid duplication of efforts and enhance data protection measures. In addition, it is common practice for organizations to engage in the cross-border transfer of personal information to their international subsidiaries, and in the context of a possible sale of the business. The transfer of employee data across borders for processing and storage often makes good business sense and in many cases cannot be avoided. However, the transfer of employee personal information, especially to third parties outside of Canada's borders, must be carefully organized and appropriate measures to protect such personal information must be established.

This article will focus on measures that organizations in Ontario can implement when proposing to transfer information to third parties outside of Canada, and is meant to serve as an introduction to some of the issues businesses should consider before engaging in the cross-border transfer of personal employee data.

(A) APPLICATION OF PIPEDA

Unlike Alberta, British Columbia and Quebec, Ontario has not implemented its own private sector privacy legislation. Accordingly, in Ontario the Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5 ("PIPEDA") governs the collection, use and disclosure of employee data by private sector organizations.

To determine the applicability of PIPEDA, counsel should consider: 1) whether the employee data at issue constitutes personal information and/or personal employee information;[2] 2) whether the disclosure of employee data occurs in the course of commercial activity;[3] and 3) whether the

---

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No.107-56, 115 Stat. 272 (2001).

[2] Pursuant to ss.2 (1) of PIPEDA, "Personal Information" means information, recorded or otherwise, about an identifiable individual, with the exception of the name, title, business address or business telephone number of an employee of an organization.

[3] "Commercial Activity" under PIPEDA is defined as any particular transaction, act or conduct or any regular course of conduct that is of a commercial character. Case law indicates that, in its ordinary meaning, "commercial activities" refer to purposes related to trade and the buying and selling of commodities. Arguably, the transfer of employee data for the purpose of administering an employer/employee relationship does not appear to constitute commercial activity, as such is defined pursuant to PIPEDA.

organization is subject to federal or provincial authority.[4] PIPEDA will be applicable where the collection, use and disclosure of personal information, including employee information, is transferred across provincial or national borders in the course of commercial activity. Although PIPEDA does not specifically define "Personal Employee Information," private sector privacy legislation from Alberta[5] and British Columbia[6] suggests that "Personal Employee Information" is personal information required by an organization to establish, manage or terminate an employment relationship. It is likely that this information would include such things as an individual's name, health care insurance number, employee number and information about a person's medical or educational history.

(B) FORM OF CONSENT

Privacy legislation is primarily consent-based. The most effective way to prevent a privacy complaint is to obtain the express consent of the individual whose personal information is subject to disclosure. Where this approach is not practical, organizations should ensure that they provide clear notification to their employees when planning to transfer and disclose employee data to third parties outside of Canada for processing and storage.

Organizations should also revise and re-distribute their employee privacy policies to account for changes to the storage of employee data, and to ensure notice and transparency in this regard. Employees should be notified in a manner which indicates the type of personal information that is at issue and should be informed of the purposes for which their employer wishes to disclose their personal information to a third party. This notification should include a method for the employee to contact his or her employer, including a telephone number or e-mail address of the designated contact person or privacy officer, to inquire about the disclosure of their personal information. It is also recommended that employees be informed about the possible risk to their personal information when it is transferred outside of Canada.[7]

(C) PROCESSING CONTRACTS WITH THIRD PARTIES

Under PIPEDA, an organization is responsible for personal information in its possession, custody or control, including information that has been transferred to a third party for processing. Accordingly, it is the responsibility of the originating organization to use contractual or other

---

[4] If an organization carries on a "federal work, undertaking or business," only then will PIPEDA apply in respect of the personal information of its employees that it collects, uses or discloses (a.4(1)(b)).

[5] Pursuant to ss.1 (j) of Alberta's Personal Information Protection Act, S.A. 2003, c.P-6.5, as amended S.A. 2005, c.29, "Personal Employee Information" means, in respect of an individual who is an employee or a potential employee, personal information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing or terminating an employment or volunteer relationship between the organization and the individual that is unrelated to that relationship.

[6] Pursuant to ss.1 of British Columbia's Personal Information Protection Act, S.B.C. 2003, c.63, as am. "Personal Employee Information" means personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and the individual, but does not include personal information that is not about an individual's employment.

[7] See Findings of the Office of the Privacy Commissioner of Canada in "Commissioner's Findings – PIPEDA Case Summary #313: Bank's Notification to Customers Triggers Patriot Act Concerns," online at http://www.privcom.gc.ca/cfdc/2005/313_20051019_e.asp. For example, the personal information of Canadians transferred to the United States is impacted by the U.S.A. Patriot Act.

means to provide a comparable level of protection while the information is being processed by a third party. The federal Office of the Privacy Commissioner has endorsed contract terms which include: 1) guarantees of confidentiality and security of personal information; 2) oversight, monitoring and auditing of the services being provided; and 3) details pertaining to the third-party service provider's security policy.[8]

For more information on this topic, or any other legal topic relating to corporate, privacy or technology law, please do not hesitate to contact the author, Candice Teitlebaum, at 416.865.4743 or cteitlebaum@airdberlis.com.

*Candice Teitlebaum is an associate and belongs to the Corporate/Commercial Group and Technology Industry Team.

The author acknowledges the assistance of Ian Mathany, a student-at-law at Aird & Berlis LLP, for his contribution to this article.

[8] Ibid. In this instance, the third-party's security policy included "administrative, technical and physical protections to safeguard against, inter alia, unauthorized usage, modification, copying, accessing or other unauthorized processing."