WHOSE E-MAIL IS IT? UNIVERSITY DOES NOT CONTROL PERSONAL E-MAIL OF FACULTY MEMBERS

Eileen E. Vanderburgh
Partner
Alexander Holburn Beaudin + Lang LLP

Who controls the personal e-mail of public body employees on the public body's e-mail system? Under public sector information and privacy legislation, all records (including e-mail) that are in the custody of or under the control of the public body are subject to provisions granting access rights to the public. This issue has been highlighted by a series of orders from provincial Information and Privacy Commissioners, considering the status of e-mail files of faculty members at Canadian universities who were involved in grant approval decisions of the Social Sciences and Humanities Research Council ("SSHRC"). Most recently, the Alberta Court of Queen's Bench[1] overturned a decision of an adjudicator delegated by the Alberta Commissioner who had found that the e-mail communications between a faculty member at the University of Alberta and the SSHRC were under the control of the University and were, therefore, subject to the access provisions in the Alberta *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25.

The adjudicator found that the University of Alberta had custody or control over the e-mail, because the e-mail would have "passed through its servers" and because the faculty members' service to the SSHRC was part of the faculty members' responsibilities to the University, thereby providing the University with authority to deal with the e-mail. The adjudicator relied on earlier decisions of the Ontario Commissioner involving e-mails between faculty members at Wilfred Laurier University[2] and the University of Ottawa[3] and SSHRC in support of her conclusion that the e-mail was in the custody of or under the control of the University of Alberta and, therefore, subject to *FIPPA*.

The Court found that the adjudicator's decision was unreasonable on three interrelated grounds. The first and overriding error, identified by the Court, was the failure of the adjudicator to consider the purpose of *FIPPA* in her interpretation of custody and control and her application of the potential relevant factors to the facts. The adjudicator failed to consider what factors in determining custody and control were relevant to assessing the connection between disclosure of the e-mail and facilitating democracy or government accountability and transparency. The Court found that the adjudicator's uncritical application of factors related to the University's right to "deal with the records," in the absence of any consideration of whether those factors related to the democratic purpose of *FIPPA*, was unreasonable.

The Court also found that the adjudicator should have recognized that the SSHRC is subject to federal access and privacy legislation and, unlike the University, exerted specific control over the e-mail. The Court commented that it was inappropriate to find that records are under the control of different organizations, subject to separate legislative regimes. Lastly, the adjudicator failed to apply relevant factors, established in previous cases, to determine custody and control, and relied on irrelevant factors. The adjudicator turned a question of the University's "right to possess the record" into the "'right to deal with the records." The Court found that a public body's routine back-up of records on a server, or monitoring e-mail in "extraordinary circumstances of breaches of ethics or law" is not equivalent to a right to possess a record. The right of a public body to possess a record includes, at the least, a right to access and use the record for its own use.

The Court relied on the Ontario Divisional Court decision in *City of Ottawa v. Ontario (IPC)*,[4] which found that personal e-mail on the City's e-mail server was not in the custody or under the control of the City for the purposes of access under the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56. The Court then concluded that the University of Alberta did not have possession of the e-mail correspondence between its faculty members and SSHRC, likening the personal e-mail to personal possessions: "Employees may keep private items at the place of work without them falling within the employer's possession and custody."

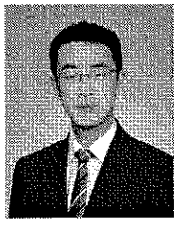
[*Editor's note*: A version of this article was originally posted on AHBL Information and Privacy Law Blog, dated May 10, 2012.]

1 *University of Alberta v. Alberta (Information and Privacy Commissioner)*, [2012] A.J. No. 393, 2012 ABQB 247.
2 *Wilfred Laurier University*, Order PO-2836 (Ontario IPC, October 28, 2009).
3 *University of Ottawa*, Order PO-2842 (Ontario IPC, November 10, 2009).
4 *City of Ottawa v Ontario (IPC)*, [2010] O.J. No. 5502, 2010 ONSC 6835.

U.S. ZIP CODE RETAILER COLLECTION CASES—ARE THEY POSSIBLE IN CANADA?

Paul Armitage
Partner
McCarthy Tétrault LLP

Jane A. Langford
Partner
McCarthy Tétrault LLP



Roland Hung
Associate
McCarthy Tétrault LLP

A recent spate of lawsuits filed in the U.S. has questioned the practice of retailers collecting zip codes in order to complete credit card transactions. The scenario is familiar: while a customer is paying for a purchase with a credit card, the cashier asks the customer for his or her zip code. The customer provides the information thinking it is somehow necessary to complete the transaction. The cashier types the zip code into the cash register and the transaction is completed seconds later without further mention of the zip code.

I. Recent U.S. Class Action Lawsuits

In the class action lawsuit *Pineda v. Williams-Sonoma Stores Inc.*[1] [*Pineda*], the Supreme Court of California held that this practice was a violation of California's *Song-Beverly Credit Card Act of 1971* [*Act*], which, in s. 1747.08, prevents retail merchants from requesting or requiring personal identification information from cardholders and recording it upon the credit card transaction form or otherwise. The Court reasoned that the zip code was the customer's personal information, that collecting it was unnecessary to complete the transaction, and that the collection was contrary to the *Act*'s intent of providing robust consumer protections by prohibiting retailers from soliciting and recording information about the cardholder that is unnecessary to the credit card transaction.

In the wake of *Pineda*, multiple class actions and lawsuits against the practice have been filed in California and elsewhere in the U.S. For example in *Akel v. Office Depot Inc., et al.*,[2] the plaintiffs brought a putative class action claiming Office Depot illegally collected customers' ZIP codes when they made purchases with their credit cards. The Plaintiffs provided Office Depot with their ZIP codes because they thought it was necessary to complete the transaction. When Office Depot moved to have the action dismissed, its motion was denied.

The rash of California ZIP code litigation continued with *Amelia Foos v. Ann, Inc. d/b/a AnnTaylor Retail, Inc.*,[3] *Bradach v. Sunglass Hut Trading, LLC*,[4] and *Wood v. Lucky Brand Dungarees Stores, Inc.*,[5] where the Plaintiffs alleged that, as a condition of using their credit cards, the respective retailers required them to provide their ZIP code. All of the