l'Association canadienne du droit
des technologies de l'information

March 21, 2012

IT.Can NEWSLETTER

Canadian IT Law Association

www.it-can.ca

This newsletter is prepared by Professors Robert Currie and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School, and David Fraser.

Les auteurs du présent bulletin sont les professeurs Robert Currie et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie, et David Fraser.

CRTC Finalizes Anti-Spam Regulations

The CRTC has released its finalized *Electronic Commerce Protection Regulations* pursuant to what is normally called "Canada's Anti-Spam Law" (here), after a period of consultation following its controversial draft regulations of July 2011. The regulations are geared towards "commercial electronic messages," and essentially provide the specifications of messages which will comply with the Anti-Spam Law and not constitute spam.

Section 2 of the Regulations deals with "Information to be Included in Electronic Commercial Messages," specifying that each message must contain: the name or business name of the sender, or the name of the entity on whose behalf the message is sent; and the mailing address and either a telephone number, e-mail address or web address of the sender or entity on whose behalf it is sent (a change from the earlier version, which required more contact information). This information may also be set out at a web link which is displayed "clearly and prominently" in the message itself. Section 3, "Form of Commercial Electronic Messages", requires that the information in section 2 and the unsubscribe mechanism (set out in s. 6 of the Anti-Spam Law itself) be set out "clearly and prominently" and that the unsubscribe mechanism "must be able to be readily performed" (a change from the earlier version, which specified "two clicks" or the equivalent).

Section 5, "Information To Be Included in a Request for Consent", sets out that requests for consent to commercial electronic messages can be sought orally or in writing (a change from the former version, which required written consent), and must include the identity-related information provided for in section 3 and a statement that "the person whose consent is sought can withdraw their consent." Section 5, "Specified Functions of Computer Programs," refers to subsection 10(5) of the Anti-Spam Law, which sets out various functions of computer programs which a sender might wish to be installed on a customer's computer and requires explicit consent regarding these various functions (e.g. collection of information stored on the customer's computer, changing settings, preferences or commands without the customer's knowledge, etc.). Section 5 specifies that these computer functions must be brought to the attention of the person from whom consent is sought "separately from any other information provided in a request for consent" and requires written acknowledgment from the person that they understand and consent to these functions.

Expert commentary here and here.

Federal Privacy Commissioner Continues to Engage Google About Privacy Policy

On 1 March 2012 Privacy Commissioner of Canada Jennifer Stoddart published a letter she sent to Google's Manager of Global Public Policy, as part of an ongoing dialogue with the company about its new privacy policy. In a letter dated 23 February 2012 Commissioner Stoddart raised a number of concerns regarding the new policy, to which Google responded on 29 February 2012. In her March 1 letter the Commissioner expressed "the view that your reply did not fully address our concerns." The original letter had asked Google to explain its policies and practices regarding retention and disposal of person information, noting that the policy was not specific. In its reply, she felt, Google did not "indicate whether Google was changing its retention policies nor did you define what the 'reasonable period of time' (after which information is deleted at

the user's request) that you noted in your letter." The Commissioner urged Google to be clear and specific on this point in its policy.

The 23 February letter had also raised issues around the linking of Google accounts, and Google's 29 February reply had "clarified how individuals can use various tools to limit ads and tracking, as well as the means of setting up separate accounts to limit personalization." However, the Commissioner expressed her concern that this information was not set out in the policy—not to mention that the policy did contain wording to the effect that linking across separate accounts could occur. She urged clarity in the policy and the addressing of this inconsistency.

Finally, she dealt in some detail with Google's clarification of how the policy dealt with Android users, noting that users could access nearly all of the device's functions without having a Google account, though some applications (Android Market, Gmail) did require the user to be logged in to a Google account. Other e-mail applications could be run on the Android. Google had noted that users logged in to a Google account had some control over how Google uses their information, in a manner similar to using a browser on a desktop. The Commissioner responded:

> It appears that an Android user, to some degree, does have some options available to protect his or her privacy. However, it is possible that you might be overstating the impact of the user's ability to delete search history (which applies to desktop users as well), including the ability to use incognito mode in the browser. None of these practices prevent the collection or retention of the search history by Google; it just means that there is no local record (on the phone or on the desktop computer) of the browsing.

She noted, however, that these latter concerns were not unique to Google. She urged Google, as with other Internet companies, to work towards improved practices in allowing opting-out from data collection, and the destruction or de-identification of information collected.

Privacy Commissioner addresses safeguarding of video surveillance records

In finding 2009-022, the Privacy Commissioner of Canada addressed a complaint that a retail store had unlawfully disclosed surveillance video recordings to her former husband's spouse and had refused the complainant's access request.

The complainant, a police officer, visited a retail establishment with another police officer. Both were surveilled by a plainclothes loss-prevention officer and by use of the store's video system. The unusual surveillance was said to be because there was a fear that the complainant had gone to the store to harass an employee, who was currently married to the complainant's ex husband. A copy of the recording was subsequently provided to that employee. Still images from the video were then used as part of a complaint to the police against the complainant. The complainant then made a request for access to the recording and was denied.

In response to the complaint, the respondent store said that this was not within the Commissioner's jurisdiction, as all of it stemmed from the employment of the individual rather than as part of commercial activities. The Commissioner did not agree with this submission.

The Commissioner did find that the respondent was justified in refusing to provide access to the recording:

> 22. Paragraph 9(3)(c.1) of the Act provides that an organization is not required to provide access to his or her personal information to an individual if the information was collected under paragraph 7(1)(b) of the Act. There are two aspects of section 7(1)(b) the Respondent must satisfy for this exception to apply. First, the collection must be reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province. Second, it must be reasonable for the Respondent to expect that collecting the information with the knowledge or consent of the individual would compromise the availability or the accuracy of the information.

On the complaint regarding the disclosure of the recording to the employee, the Commissioner found that this was contrary to PIPEDA: "Organizations must not disclose, without consent, third-party personal information to an employee for that employee's personal purposes unless it is very clear that an exception to consent applies."

Privacy Commissioner criticizes Canadian social networking site

In response to a wide-ranging complaint from the Public Interest Advocacy Centre, the Privacy Commissioner of Canada has completed its investigation into the Canadian based Nexopia social networking site principally focused at youth and young adults and has publicly released her report of findings.

The Commissioner found that Nexopia was in violation of the *Personal Information Protection and Electronic Documents Act* in four principal areas:

- Default settings that were particularly inappropriate for Nexopia's target youth audience, and a lack of clarity about available privacy settings;
- A lack of meaningful consent for the collection, use and disclosure of personal information collected at registration;
- The sharing of personal information with advertisers and other third parties without proper consent; and
- The indefinite retention of personal information.

The investigation led to 24 recommendations, most of which the site followed. Notably, the site would not fully delete users' accounts even after users asked to have them deactivated and deleted. Among the reported reasons for not doing so was the desire to preserve the information in case law enforcement was interested in the data.

On the outstanding issues, the Commissioner stated in her news release that she is considering her options, including a proceeding in Federal Court.

US University Student Found Guilty of Webcam Crimes

On March 16th, former Rutgers University student Dharun Ravi was convicted on fifteen criminal charges arising from his use of a webcam. The much-publicized case stemmed from the September 2010 suicide of Tyler Clementi, a gay teenager and Ravi's roommate at Rutgers. Clementi leapt from the George Washington bridge after discovering that Ravi had surreptitiously filmed and broadcast Clementi's romantic encounter with another man. Ravi was convicted of a number of counts described in media reports as "hate crimes," including "bias intimidation," and also of invasion of privacy. Having been asked by Clementi for some private time in their dorm room, Ravi turned on a webcam he had secretly installed in the room and tweeted a number of times about having viewed Clementi having an encounter with another man. A number of students viewed a live-streamed feed from the webcam. Clementi viewed Ravi's Twitter page 38 times during the two days before he committed suicide.

CDRP panel finds against registrant who claimed it was registered on behalf of unnamed customer

In dispute number DCA-1358-CIRA, the French company that manufactures Cointreau liquors objected to the registration of the domain name cointreau.ca by a Prince Edward Island registrant, Netnic Corporation. The respondent alleged that it had registered the domain name for an unnamed customer and was holding onto the registration in order to secure payment.

The respondent did not lead any substantial evidence regarding the purpose for the registration, or even who the customer was alleged to be. In light of a range of "COINTREAU" trade-marks held by the applicant in Canada and correspondence with a representative of Netnic, the applicant was able to convince the panel that the trade-mark was confusingly similar to a mark in which the applicant has rights, that the registrant did not have any legitimate interest in respect of the domain name.

Finally, the panel concluded that given the representative or "alter ego" of the registrant had previously lost a number of domain name disputes and was engaged in a pattern of abusive registrations. In the result, the domain name was ordered transferred to Cointreau.

Nova Scotia Cyberbullying Task Force releases its report

The Nova Scotia Task Force on Bullying and Cyberbullying has released its report, entitled "Respectful and Responsible Relationships: There's No App for That".

The Task Force was struck in April 2011 in response to two instances of youth suicide that parents said stemmed from online harassment and bullying. The report includes 85 recommendations, including the appointment of a provincial anti-bulling coordinator, progressive discipline in classrooms for bullying and an annual conference on the subject.