Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télec.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

AUG 07 2008

Files: 6100-02681, 6100-02682, 6100-02683

Ms. Philippa Lawson
Executive Director
Canadian Internet Policy and Public Interest Clinic
Faculty of Law
University of Ottawa
57 Louis-Pasteur
Ottawa ON K1N 6N5

Dear Ms. Lawson:

Please find attached the report of findings prepared by this Office with regard to the complaints you filed against Canada.com under the *Personal Information Protection and Electronic Documents Act* (the *Act*), and received by our Office on August 1, 2007.

Following the investigation into your complaints, I have concluded that the matter is not well-founded. For details on the investigation and the rationale for my conclusion, please see the attached report of findings.

Now that you have my report, I must inform you that, pursuant to section 14 of the *Act*, you have the legal right to apply to the Federal Court of Canada if you wish to pursue this matter any further.

Should you wish to proceed to Court, we suggest you contact the Court office nearest you. Normally, an application must be made within 45 days of the date of this letter. For additional information on Federal Court applications, please check the Fact Sheet, Application for Court Hearings under PIPEDA, found on this Office's web site at http://www.privcom.gc.ca/fs-fi/02_05_d_31_e.asp.

This concludes this Office's investigation of your complaints. If you have any questions or comments about the disposition of the complaints, I would invite you to contact Trevor Yeo, Privacy Investigator, at 1-800-282-1376.

Sincerely,

Elizabeth Denham
Assistant Privacy Commissioner

Attachment

Report of Findings

Files: 6100-02681
6100-02682
6100-02683

Complaints under the *Personal Information Protection and Electronic Documents Act* (the *Act*)

1. The complainant alleges that canada.com did not obtain customer consent to disclose sensitive personal information of e-mail subscribers to a third-party U.S.-based e-mail provider.

2. The complainant also alleges that canada.com does not provide adequate notice to new customers of the information disclosure/transfer to the U.S.-based provider.

3. The complainant also claims that the level of protection of personal information provided by the U.S.-based service provider is not comparable to that which would be provided by businesses operating within Canadian borders.

Summary of Investigation

4. According to the complainant, on February 20, 2007, canada.com sent an e-mail to its e-mail subscribers, stating that e-mail services would henceforth be operated by a company based in the U.S. With no mention of obtaining the prior consent of subscribers, the e-mail also advised that all previously saved messages, folders and settings would automatically be transferred to the new account. Our Office examined a copy of that e-mail.

5. The e-mail continued that upon logging in to their new account, subscribers would be asked to accept or decline the new services. If subscribers declined, their e-mail account and all its contents would be permanently deleted.

6. The complainant asserts that new subscribers to canada.com e-mail services must provide their agreement with the company's terms and conditions, as well as with its privacy statement. The complainant notes that the terms and conditions point out that e-mail services are provided by a third party located in the U.S. and that, as such, the disclosure of subscriber personal information stored in that location is subject to foreign laws.

.../2

7. According to the complainant, the frequently asked questions (FAQs) document produced by canada.com states the following:

> *... information processed or stored outside of Canada may ... no longer falls under the jurisdiction of Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") nor be subject to canada.com's Privacy Statement ....*

8. The complainant included in her representations copies of canada.com's website home page, the FAQs page, registration page, privacy statement and the terms and conditions document.

9. The complainant also cites an e-mail dated March 29, 2007, from the legal representative of canada.com to a canada.com e-mail subscriber in which the subscriber was advised that under the contractual agreement between canada.com and the U.S.-based e-mail provider, the provider was obligated to comply with privacy laws "... to the extent that they do not conflict with American Laws."

10. In its representations, the respondent first explained that canada.com is an interactive web portal owned and operated by CanWest, and that the e-mail services have always been provided by various third parties since 1998. (Since 2006, its e-mail service providers have operated from the U.S.) Moreover, from the respondent's point of view, the movement of client information to the third party does not constitute a *disclosure*, but rather an information *transfer*.

11. With regard to CanWest obtaining the consent of existing subscribers in early February 2007 for the purpose of transferring their personal information for e-mail services, the company contends that the necessary consent had previously been obtained when these subscribers originally signed up for canada.com e-mail. Although the third-party service provider may have changed in February 2007, the *purpose* of the third-party information transfer has remained constant and, thus, subscriber consent did not require renewal. CanWest notes that this position is in keeping with the findings of PIPEDA case summary #313.

12. Moreover, CanWest contends that, because the data was fragmented and some of it was still stored in Canada, no personally identifiable information of existing subscribers was ever transferred to the new, U.S.-based provider until subscribers had clearly consented to it.

.../3

13. The company provided our investigation with a description of what would happen during the first login for existing e-mail subscribers on and after February 28, 2007 (i.e. the "go live" date for the new service): First, a subscriber login would be re-directed from Canada to the third-party's servers in the U.S., where partial data (i.e. subscriber e-mail message content, passwords and usernames) awaited activation, having previously been transferred and stored there. The usernames were stored on separate servers from the message content. Meanwhile, the full name and address of subscribers ("account information") remained on canada.com servers in Canada, where the respondent claims that it has always been stored.

14. Since the subscriber data was still in raw format, CanWest did not consider it to be personally identifiable information at this point.

15. Upon receipt of the login, the third-party servers would then send an electronic message to the canada.com servers in Canada, asking for authentication of the user. Subscribers were then informed by way of a pop-up window of the new service provider in the U.S. (identified by name) and that, until they logged in and accepted the terms and conditions and the CanWest privacy statement, any of their e-mail content and username information would not be activated and could not be accessed by any third party.

16. If subscribers indicated their agreement, the server in Canada sent an "authentication ticket" to the U.S.-based server, which synchronized subscriber e-mail content information with the username. According to the respondent, in the event that a subscriber declined the new service, the account would be immediately and permanently deleted from the U.S.-based servers. After 90 days of the "go live" date, inactive accounts were also permanently deleted from these servers.

17. Concerning new subscribers' consent, they must also accept the company's privacy statement. CanWest also currently informs them in its terms and conditions (updated on February 28, 2007) of the following:

> *You acknowledge that in the event that a third party service provider is located in the United States or another foreign country, your personal information may be processed and stored in the United States or such other foreign country, and the governments, courts or law enforcement or regulatory agencies of that country may be able to obtain disclosure of your personal information through the laws of the foreign country.*

.../4

18. This information is also available in its "Frequently Asked Questions" (FAQs) document, available on the canada.com website, which clearly states that canada.com e-mail is provided by "...a company located in and conducting its business from the United States."

19. The respondent conceded to this Office that its FAQs document originally misrepresented the jurisdictional powers of the *Act* for personal information collected in Canada and transferred to another country. This erroneous information was also communicated to subscribers in the pop-up window that appeared (as a reminder) simultaneously with each e-mail login/sign up for approximately one week after subscriber agreement was obtained. It read as follows:

> *... information processed or stored outside of Canada may ... no longer fall under the jurisdiction of Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") nor be subject to canada.com's Privacy Statement ....*

20. On March 14, 2007, the FAQs document was revised as follows:

> *... the information processed or stored outside of Canada may be available to the foreign government of the country in which the information or the entity controlling it is situated under a lawful order made in that jurisdiction.*

21. The respondent also concedes that it erroneously advised the complainant in an e-mail dated March 29, 2007, that under the contractual agreement between the two parties, the third party provider was obligated to comply with privacy laws "... to the extent that they do not conflict with American Laws." CanWest has reviewed its message and now claims that the signed agreement does not, in fact, contain any statement worded in such a manner. Rather, the intended message to the complainant was to convey the following:

> *... while customer personal information is in the hands of a foreign third-party service provider, it is subject to the laws of that country and no contract or contractual provision can override those laws. (PIPEDA case summary #313)*

.../5

22. With regard to the level of personal information safeguarding required of the U.S.-based third party by CanWest, the respondent provided our investigation with a copy of the signed agreement between the two parties, as well as four particular confidentiality items with which the third party must comply. The agreement stipulates that the third party must process the subscriber data in compliance with both CanWest's privacy policy and the *British Columbia Personal Information Protection Act* (PIPA). PIPA is deemed to be substantially similar privacy legislation with respect to the *Act*.

23. In addition, CanWest responded that the third party has in place strict technical requirements for the storage and processing of subscriber data (including separate storage of the e-mail content and user information) and for hosting the directory on a Uniform Naming Convention file share so as to disable text-based file queries. The U.S.-based servers are located in a 24-hour-secure date center, accessible only by authorized personnel.

24. Lastly, the respondent addressed the issue of the disclosure of personal information without consent within the contexts of the *USA Patriot Act* and privacy laws. CanWest contends that, notwithstanding the storage location of personal information data—for example, in Canada or the U.S.—the *Act* does not preclude disclosures to government institutions without an individual's consent. By way of example, CanWest cited paragraphs 7(3)c, 7(3)c.1, 7(3)c.2 and 7(3)l of the *Act*, which describe particular circumstances involving governmental or legal authorities under which knowledge and consent of the individual are not required to disclose her or his information. In light of these provisions, the respondent states that "… government access without consent will always remain a possibility, both in Canada and in the United States."

25. Responding to the notion that the *USA Patriot Act* more readily allows access by U.S. authorities to Canadians' personal information—when compared to other statutes and information-sharing agreements—CanWest states the following:

> *While it is within the power of an organization to set forth contractual and operational controls on the treatment of personal information by its service providers, it is unreasonable to expect organizations to conduct exhaustive surveys of data access statutes in every jurisdiction in which they process or store data and make a determination whether or not those statutes put the data at greater risk than they would if situate [sic] in Canada. We submit that such a standard goes beyond the spirit and intent of PIPEDA, particularly the reasonableness standard set forth in Section 3.*

…/6

Application

26. In making our determinations, we applied Principles 4.1.3, 4.3, and 4.3.2, of Schedule 1 of the *Act*.

27. Principle 4.1.3 states that an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

28. Principle 4.3 states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

29. Principle 4.3.2 clarifies that the principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information shall be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

Findings

30. At issue in the first place is whether canada.com e-mail subscribers were provided with an opportunity to consent to the sharing of their personal information with the third-party e-mail provider.

31. This Office has taken the position in previous findings that the sharing of information with a third-party service provider constitutes a "use" for the purposes of the *Act*, and that an individual's consent must be obtained for the uses of her or his personal information. In my view, CanWest obtains customer consent for the use of personal information for the provision of e-mail when subscribers first sign up for canada.com e-mail services. Although the service provider has changed over time, the purpose of the current provider's use of the personal information has remained the same. Thus, the respondent was not required to obtain customer consent for the information use when the new provider took over the service in February 2007.

.../7

32. Nonetheless, this Office's investigation has demonstrated that, at the time of the transfer of information to the new service provider, both new and existing customers were informed directly of the new arrangement (by e-mail) and were provided with a clear opportunity to consent to it by means of a pop-up box at time of login. Available supporting documents conveying the same information included the company's terms and conditions, privacy policy and the frequently asked questions (FAQs). Both the terms and conditions and the FAQs clearly advised subscribers that some information was stored in the U.S. and could potentially be accessed by a foreign government.

33. Moreover, our investigation confirmed that any data which was transferred to the new service provider prior to notification of the subscribers in February 2007 was, in fact, not accessible to any third party and could not be personally identifiable until consent was given by e-mail account holders. Consequently, Principles 4.3 and 4.3.2 were upheld.

34. The second issue is whether the level of protection of personal information held by the U.S.-based service provider is comparable to that of a Canadian-based provider.

35. I am satisfied that CanWest has maintained custody and control of the information that is processed by its third-party service provider in the U.S. The service agreement between the two parties relies on unambiguous language that provides guarantees of the confidentiality and security of personal information, and it allows for oversight, monitoring and audit of the services being provided. In my view, the contractual provisions with regard to information protection are no less stringent than they would be if the service provider were located within Canadian borders.

36. Concerning U.S. authorities' access to canada.com subscriber personal information by virtue of a Section 215 Order under the *USA Patriot Act*, CanWest cannot rely on the exceptions set out in paragraphs 7(3)c, 7(3)c.1, 7(3)c.2 and 7(3)i of the *Act*. This position is consistent with our Office's findings in case summary #313. For that matter, I do not believe it possible either for CanWest to use contractual or other provisions to override the provisions of the U.S. statute.

37. The risk of a U.S.-based service provider being ordered to disclose personal information to U.S. authorities is not a risk unique to U.S. organizations. In the national security and anti-terrorism context, Canadian organizations are subject to (and may be just as likely to receive) similar types of orders to disclose personal information of Canadians to Canadian authorities. There are also

.../8

several formal bilateral agreements in place between analogous Canadian and U.S. organizations that provide for the cooperation and exchange of relevant information. In light of such arrangements, there are many alternatives to a Section 215 Order to obtain information about Canadians.

38. Finally, organizations that outsource the processing of personal information must provide sufficient notice with respect to the existence of service-provider arrangements, including notice that any foreign-based service provider may be required by the applicable laws of that country to disclose personal information in the custody of such service provider to the country's government or agencies. In this respect, CanWest respected its obligation by reliably informing its subscribers, new and existing, of its arrangement with a new U.S.-based e-mail provider and of the potential impact on confidentiality of subscriber information. Consequently, Principle 4.1.3 was not contravened.

Conclusion

39. Accordingly, the complaints are not well-founded.