



July 25, 2007

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

Dear Commissioner:

Re: PIPEDA s.11 complaint re: canada.com email service - outsourcing to US-based service provider

This is a complaint regarding canada.com's compliance with the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") in respect of the outsourcing of its email operations to a US-based service provider, Velocity. We have been alerted to this issue by a canada.com subscriber who has already filed a complaint with you about the matter. This letter sets out our analysis of canada.com's obligations under the Act, and will, we hope, assist you in your analysis of the same.

Request

We request that you investigate and report on canada.com's compliance with PIPEDA, and in so doing that you clarify:

- a) the distinction between "transfers for processing" and "disclosures" under the Act, and
- b) the notice requirements under Principle 4.1.3, and
- c) whether there is an exception to the consent requirement under Principle 4.3 for business transfers that involve no new purposes, and if so, the nature and scope of such exception.

We also request that you revisit the issue of "comparable level of protection" for customer information held by businesses in Canada versus the US, and provide a full explanation of the processes by which such information can be accessed by the US government agencies under US law, under each scenario.

Summary Conclusion

We submit that canada.com is in violation of the following PIPEDA requirements with respect to its outsourcing of email operations to a US-based company:

- ensuring a "comparable level of protection" (if Principle 4.1.3 applies);

- obtaining customer consent to disclosure of sensitive personal information (if Principle 4.3 applies); and
- providing adequate notice to new customers of the disclosure/transfer to a US-based service provider (Principle 4.8, and Principle 4.3 if it applies).

The Facts

On February 20, 2007, canada.com sent an email to current customers advising that “canada.com email will now be operated by Velocity Services Inc, a company based in the United States.” The email further advised:

The migration to our new email service will occur over the next 2 weeks...All previously saved messages, folders and settings will automatically transfer to your upgraded account...All accounts- without exception- will be transferred to this new service. Upon log-in to your email account you will be asked to accept or decline the new services being offered. Please note, if you decline, your email account including all of its contents will be deleted.

New customers signing up to canada.com must acknowledge that they “accept and agree to be bound by the Terms and Conditions...and have read and understand the Privacy Statement”, both of which are hyper-linked for ease of reference during the registration process. Canada.com’s Privacy Statement is silent as to canada.com’s potential use of foreign third party service providers, as well as to the ramifications of this foreign outsourcing. However, the Terms and Conditions do address outsourcing to third parties and the implications of such as follows:

- a) *Terms and Conditions-Term 24: “Third Party Dealings & Online Sales Disclaimer”*
 You acknowledge that some of the services accessible on the canada.com Site are provided by third parties...You acknowledge and agree that canada.com email services are made available by Velocity Services, Inc. (“VSI”) pursuant to the terms provided when registering for canada.com email services, and your use of canada.com email services is governed by VSI’s End User Terms and Conditions available here [hyper-link provided]. You acknowledge and agree that canada.com shall have no responsibility for, or liability with respect to, any aspect of the canada.com email service.

Terms and Conditions-Term 3: “canada.com Privacy Statement”

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. Whenever we engage a third party service provider to do work for us, we

confirm that its privacy and security standards meet our requirements. You acknowledge and agree that this paragraph constitutes prior written notice to you of, and your consent to the collection, use and disclosure of your personal information as described above.

Canada.com's Privacy Statement and Terms and Conditions of use are also accessible to anyone browsing the site via small-print links at the bottom of every page. Also accessible in this manner is a set of Frequently Asked Questions ("FAQs"), which include the following question and answer:

FAQ: where will my canada.com email account information be stored?

canada.com email (the "Service") is provided by Velocity Services, Inc. ("VSI"), a company located in and conducting its business from the United States. By registering for and/or logging on to the Service, you accept and acknowledge that 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 *and 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.* [Note: canada.com has since updated its FAQ and removed the italicized references to PIPEDA and the suggestion that the canada.com Privacy Statement no longer applies.]

Attached are print-outs of canada.com's home page (in 3 pages as it would not fit on one page), FAQ page, relevant FAQ, registration page, Privacy Statement, and Terms and Conditions of July 25, 2007.

In an email message sent to a subscriber on March 29, 2007, Andre Desautels, Legal Affairs for CanWest Global, stated: "VSI has agreed contractually to comply with Canadian privacy laws to the extent that they are not conflicting with American laws...Both the new service provider and canada.com employ up-to-date technologies in terms of restricting and securing access to information on our servers."

Analysis

In order to identify canada.com's obligations under PIPEDA with respect to its outsourcing of email services to Velocity, it must first be determined whether such outsourcing constitutes a "disclosure" under Principle 4.3 of PIPEDA (in which case consent is required, unless "inappropriate"), or instead a mere "transfer for processing" under Principle 4.1.3 (in which case consent is not required, but some notice still is). The former applies if canada.com gives up custody and control of the data once sent to Velocity; the latter applies if Velocity is simply acting as canada.com's agent. The facts in the case suggest both: on one hand, canada.com is disclaiming responsibility for the data once it is sent to Velocity and is purporting to obtain consent from customers to this

disclosure. On the other hand, canada.com continues to be the service provider of record and Velocity seems to be acting as its agent. Canada.com's obligations regarding notice and consent depend on which provision applies.

Because it is not clear from the available facts which Principle governs the actions of this case, we address canada.com's obligations under both of these provisions.

Scenario #1: Transfer for Processing

4.1.3- *“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.”*

Comparable Protection

Assuming that Principle 4.1.3 applies in this case, canada.com is under a legal obligation to ensure that Velocity provides “a comparable level of protection” to its customers' data as canada.com is required to provide under PIPEDA. We submit that the mere outsourcing to a US company lowers the level of protection provided to canada.com email customers because of the vulnerability of US companies to enforceable demands by the F.B.I. for customer data under the *Patriot Act*.

Even if the contract between canada.com and Velocity [VSI] requires VSI to provide a comparable level of protection for the information, canada.com cannot stop VSI from disclosing its customers' email information to US authorities in response to US subpoenas or court orders, even if such orders would not be enforceable in Canada. As indicated in the March 29, 2007 email sent by Andre Desautels, from Legal Affairs for CanWest Global: “VSI has agreed contractually to comply with Canadian privacy laws *to the extent that they are not conflicting with American laws...*” (emphasis added).

We understand that you have found in a past case that “there is a comparable legal risk that the personal information of Canadians held by any organization and its service provider — be it Canadian or American — can be obtained by government agencies, whether through the provisions of US law or Canadian law”, given the “longstanding formal bilateral agreements between the US and Canadian government agencies that provide for mutual cooperation and for the exchange of relevant information.” (Case Summary #313)

We challenge your finding that bilateral agreements between Canada and the United States represent a comparable risk to individual privacy as do the provisions of the *US Patriot Act*. While we have not conducted a thorough comparison of the relevant laws and agreements, it is our understanding that the *Patriot Act* allows for much easier and faster access by US authorities to Canadians' personal information than is the case under other existing laws and information-sharing agreements. If this is not the case, we would appreciate understanding exactly how FBI demands for customer information (e.g.,

subscriber lists, email communications) from a Canadian organization would be processed and enforced through the “longstanding formal bilateral agreements” referred to above.

Notice

Although Principle 4.1.3 contains no notice provision, Principle 4.8 applies, requiring openness by the company about its information management practices (see below). In past PIPEDA complaints involving transfers for processing, the Office of the Privacy Commissioner has taken the position that compliance with Principle 4.8 will be assessed on the basis of whether organizations have informed customers that third party processing occurs and of the corresponding law-enforcement-access ramifications. For instance, PIPEDA Case Summary #365 (with almost precisely the same wording utilized in PIPEDA Case Summary #313) states:

at the very least, a company in Canada that outsources information processing to a company that operates in another country should notify its customers that the information may be available to the government of that country or its agencies under a lawful order made in that country.

In both Case #313 and #365 it was determined that because such information was provided, adequate notification was given to meet Principle 4.8. In Case #313, the bank sent a notice to customers via a bill insert, specifying that it was now using a US-based service provider and informing customers of the risk that their personal information might be accessed under the provisions of the US *Patriot Act* while in the hands of the US-based third party service provider. In Case #365, on the other hand, no individual notices were sent. Rather, the banks relied upon their publicly available privacy policies to inform customers that they used third party processors, some of which may be located outside of Canada. These policies stated that while customer information is outside of the country, it is subject to the laws of the country in which it is held.

In the case of *canada.com*, *existing* customers were specifically informed of the disclosure to a US-based company (though not of the *Patriot Act* risks) via an email.

New customers, however, do not receive such notice. Instead, they are required to indicate their consent to *canada.com*'s Privacy Statement and Terms and Conditions of service, both of which are accessible from the *canada.com* website. Term 24 of the Terms and Conditions of service notifies customers that email services are provided by Velocity, but does not state that Velocity is US-based. *Canada.com*'s Privacy Statement, surprisingly, says nothing about the outsourcing to Velocity. In order to understand clearly that their email will be transferred to a US company and will therefore be vulnerable to US law enforcement access under US laws, new customers must not only read through the Terms and Conditions of service, but must also seek out and read the company's FAQs addressing this issue. Such fragmented notice does not meet the test set out by the Commissioner or required by the Act, in our view.

Even if passive notice is sufficient, the place where consumers would most likely look for this information, namely canada.com's Privacy Statement, is silent as to canada.com's potential use of foreign third party service providers, as well as to the ramifications of this foreign outsourcing. The absence of any notice in canada.com's Privacy Statement is fatal, in our view.

For these reasons, we submit that canada.com is not providing adequate notice to new customers of the fact that their email will be administered by a US-based company and will thus be subject to US laws.

Other

If 4.1.3 applies, then canada.com continues to be responsible for the personal information and cannot contract out of liability as it has purported to do in Term 24 of its Terms and Conditions of service. Should you find that this is a "transfer for processing" situation, then canada.com should be ordered to take responsibility for its customers' information held by Velocity and revise its contract with Velocity and its Terms and Conditions to customers accordingly.

Scenario #2: Disclosure

4.3- *"The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."*

Principle 4.3 applies if canada.com's outsourcing to Velocity is considered a "disclosure" as opposed to a mere "transfer for processing". It requires knowledge and consent on the part of individual customers to the disclosure of their email to Velocity, unless such consent would be "inappropriate". As canada.com attempted to get the consent of its existing customers to the transfer via an opt-in process, this does not seem to be a case where obtaining consent would be "inappropriate". Nor do any of the examples of inappropriate consent in the note under Principle 4.3 apply in this case.

Assuming that 4.3 applies, the question then is: Did canada.com get valid consent from its customers to the transfer? Valid consent requires:

1. Proper notice (knowledge requirement)
2. Proper form of consent (opt-in or opt-out) (4.3.6)
3. Timeliness of consent

1. Proper Notice

In order to be valid, consent must be informed. In this case, customers must be properly notified of the fact that their emails are being disclosed to a US-based company, Velocity. This requirement of notice to individual customers goes beyond the Principle 4.8 requirement for openness.

Canada.com may have met this requirement with respect to existing customers, to whom it sent an email on February 20, 2007 advising that “canada.com email will now be operated by Velocity Services Inc, a company based in the United States.” Existing customers were required to expressly consent to this disclosure in order to continue using the canada.com service.

However, as explained above, new customers of canada.com are not similarly informed of the disclosure to Velocity. Canada.com requires new customers to agree to its Terms and Conditions of service and its Privacy Statement, but the latter says nothing about outsourcing to US companies, and the only notice provided via the Terms is located far down in the document and is incomplete. Neither of these documents explicitly states that canada.com uses a **US-based** company to provide its email services. While canada.com’s FAQs include a Q&A indicating that Velocity is “located in and conducting business from the United States” and that “information processed or stored outside of Canada may be available to the foreign government of the country”, new customers are not directed or even alerted to the FAQs when registering for email service.

A customer concerned about her privacy, who wishes to inform herself of canada.com’s outsourcing policies prior to consenting to the email service, will reasonably look for that information in canada.com’s Privacy Statement, and should not be expected to read through all documents published by the company on its website in order to understand whether or not her personal information will be made vulnerable to covert access by a foreign government.

2. Proper Form of Consent

Under Principle 4.3, express (opt-in) consent is required where the information in question “is likely to be considered sensitive”. As your office states in its Fact Sheet entitled *Determining the appropriate form of Consent under PIPEDA*, opt-in consent means “the organization presents an opportunity for the individual to express positive agreement to a stated purpose.” The information in question here, namely email messages, is, in our view, information of a potentially highly personal and sensitive nature. Emails today are used for transmission of an extremely broad range of content and communications, often including very sensitive family, biographical and financial correspondence. Therefore, canada.com should be obtaining express consent from all of its customers before sharing their email information with Velocity.

Canada.com seems to have fulfilled this requirement with respect to existing customers, via the email it sent on February 20, 2007 to its customers stating that “upon log-in to your email account you will be asked to accept or decline the new services being offered. Please note, if you decline, your email account including all of its contents will be deleted.”

However, canada.com has not, in our view, met the requirement for express consent with respect to new customers. While new canada.com customers must provide checkmark clicks indicating they have read and accept the Privacy Statement and Terms and

Conditions, no explicit consent is obtained with respect to the specific issue of disclosure of customer's email information to American-based Velocity. The broad consent to a long list of Terms and Conditions is not sufficient to meet the consent requirement under Principle 4.3. Especially where opt-in consent is required, the disclosure to Velocity must explicitly be brought to the attention of new customers, as it was for existing customers.

3. Timeliness of Consent

While there is no explicit requirement in PIPEDA for timely consent, timeliness is clearly implicit in the requirement for consent. In reading the February 20, 2007 emailed notice from canada.com it seems apparent that canada.com transferred the saved messages, folders and other email content of existing customers to US-based Velocity before giving its customers a choice to accept or decline the new service (and thus without the prior consent of its existing customers.) Thus, it seems that adequate consent was neither asked for nor received prior to disclosure, as required by Principle 4.3

Conclusion regarding Principle 4.3

If Principle 4.3 applies, canada.com is non-compliant, in our view, as a result of:

- a) its failure to properly notify new customers of the disclosure to Velocity, and to get their express consent to such disclosure, and
- b) its disclosure the information of existing customers to Velocity prior to obtaining customer consent.

Scenario #3: Disclosure for Same Purposes

One of the noted deficiencies of PIPEDA is its failure to address situations such as business acquisitions in which customer information is transferred to a third party, but for no new purposes. In such situations, a narrow reading of the Act suggests that consent is required. However, under a broader, purposive reading of the Act it could be argued that consent is only required for new purposes. In such cases, notice may be sufficient.

Without access to canada.com's contract with Velocity, we do not know whether Velocity is using the email information for purposes other than those to which canada.com's customers originally consented. If only the location and processing company have changed, then consent may not be required, consistent with your reasoning in Case Summaries #313 and #330.

Even if this purpose-based exception to the consent requirement applies, however, canada.com must still provide adequate notice to its customers of the disclosure in question, and for the reasons set out above and below, we submit that it has failed to do so.

Openness: Principle 4.8

“An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.”

4.8.1- *“Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization’s policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.”*

Regardless of whether Principle 4.1.3 or 4.3 applies, canada.com is required to make information about its outsourcing of email operations to a US-based service provider available to individuals in a manner that does not require unreasonable effort. As noted above, one must read through the company’s Terms of service as well as its FAQs in order to understand that canada.com’s email service is administered by a US-based company and is therefore subject to access by US authorities under US law. This fragmented approach does not, in our view, meet the requirements of Principle 4.8.

Conclusion

For all these reasons, we submit that canada.com has failed or is failing to comply with Principles 4.1.3, 4.3 and/or 4.8 of PIPEDA, in respect of its outsourcing of email operations to a US-based company.

We request that you investigate and report on canada.com’s compliance with PIPEDA, and in so doing that you clarify:

- a) the distinction between “transfers for processing” and “disclosures” under the Act, and
- b) the notice requirements under Principle 4.1.3, and
- c) whether there is an exception to the consent requirement under Principle 4.3 for business transfers that involve no new purposes, and if so, the nature and scope of such exception.

We also request that you revisit the issue of “comparable level of protection” for customer information held by businesses in Canada versus the US, and provide a full explanation of the processes by which such information can be accessed by the US government agencies under US law, under each scenario.

Sincerely,

Philippa Lawson
Director, CIPPIC
plawson@uottawa.ca
613-562-5800 x2556

Shaun Gluckman
Student intern, CIPPIC
sgluckman@cippic.ca

Attach