



LAW OFFICE OF  
**KRIS KLEIN**  
*a professional corporation*

# **Applying Canadian Privacy Law to Transborder Flows of Personal Information from Canada to the United States: A Clarification**

September 2008

---

## EXECUTIVE SUMMARY

There is a lot of confusion about the application of Canadian privacy law to the flow of personal information from Canada to the United States. This paper clarifies what is and what is not permitted when transferring personal information outside of Canada for processing purposes.

**1. CANADIAN FEDERAL LAW DOES NOT PROHIBIT THE CANADIAN PRIVATE SECTOR FROM TRANSFERRING PERSONAL INFORMATION TO THE UNITED STATES.** The *Personal Information Protection and Electronic Document Act*<sup>1</sup> (PIPEDA), Canada's federal private sector privacy law, is clear that organizations that are otherwise compliant with the law's requirements are able to freely move personal information across the border if it makes business sense to do so. Findings by the Privacy Commissioner confirm this.

**2. CANADIAN FEDERAL LAW DOES NOT PROHIBIT CANADIAN FINANCIAL INSTITUTIONS FROM TRANSFERRING PERSONAL INFORMATION TO THE UNITED STATES.** The Canadian laws and Commissioner's decisions are equally clear that financial institutions may transfer personal information outside of Canada without obtaining additional consent of customers for such transfers so long as the financial institution provides notice to customers about its information practices and remains accountable for safeguarding the information.

**3. CANADIAN LAW DOES NOT PROHIBIT THE FEDERAL GOVERNMENT FROM TRANSFERRING PERSONAL INFORMATION TO THE UNITED STATES.** The *Privacy Act*<sup>2</sup>, Canada's federal public sector privacy law, like its private sector counterpart, does not prohibit the international transfer of personal information. The Treasury Board of Canada recognizes the practice is essential and cost effective in many situations and the government position is that the transfer is permitted so long as government institutions take certain precautions to ensure the personal information is appropriately safeguarded.

**4. Except in certain situations in British Columbia and Nova Scotia, CANADIAN PROVINCIAL LAWS DO NOT PROHIBIT THE TRANSFER OF PERSONAL INFORMATION TO THE UNITED STATES.** Public sector bodies and their private sector service providers located in most Canadian provinces are not prohibited from transferring personal information outside of Canada. While British Columbia and Nova Scotia have enacted legislation that limits a public body's ability to outsource, every other province's laws are clear that the transfer of personal information is permitted. Moreover, even in British Columbia and Nova Scotia, there are no restrictions on a third party service provider from *accessing* the information in Canada<sup>3</sup> and therefore the continued benefits of economy and

---

<sup>1</sup> S.C. 2000, c.5.

<sup>2</sup> R.S.C. 1985, c. P-21

<sup>3</sup> *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996 c. 165 section 30.1 and *Personal Information International Disclosure Protection Act*, S.N.S. 2006, c. 3 section 5.

efficiency from service and support arrangements remains an option.

## INTRODUCTION

In a world where the flow of personal information is crucial to business and government, the restriction on the movement of personal information increases costs, lowers productivity, dampens innovation, stunts growth, and creates barriers to commerce. As a result, both the private and public sectors have an interest in the secure, free flow of personal information that ensures, among other things, opportunities for economic growth. The Organisation for Economic Co-operation and Development (OECD) recognized this interest in its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which states that “Restrictions on these flows could cause serious disruption in important sectors of the economy”.<sup>4</sup>

The Canadian and United States governments have also officially recognized the importance of the free flow of information between the two countries. In their Statement of the Free Flow of Information and Trade in North America<sup>5</sup>, the governments jointly noted that “Cross-border data flows are an important underpinning of all international trade transactions”.

Unfortunately, when it comes to the transfer of personal information from Canada to the United States, there is a lot of confusion about *perceived* prohibitions, as opposed to *actual* prohibitions, under Canadian privacy law. This paper clarifies what is permitted and what is not permitted when it comes to transferring personal information outside of Canada for processing purposes.<sup>6</sup> It reviews what Canadian law says about cross-border personal information flows and, just as importantly, what it does not say. It also reviews Canadian government guidance and Canadian Privacy Commissioner findings about transfers of personal information to locations outside Canada. While the legal framework and government guidance discussed below apply to any transfer of personal information outside of Canada, this paper focuses on transfers of personal information from Canada to

---

<sup>4</sup> *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980. Online: [http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html)

<sup>5</sup> Mexico is also a signatory to the Statement. It was signed in February 2008 as part of the Security and Prosperity Partnership between Canada, the United States and Mexico. The Statement can be found at: <http://www.spp-ppsp.gc.ca/pdf/SPPStatement%20Free%20FlowFinal%20-%20eng-fre-spanish.pdf>

<sup>6</sup> This paper will focus on situations where organizations are contemplating a relationship where the personal information is *transferred for processing*. The difference between a transfer and a disclosure is that in a *transfer* situation, the organization that originally collected the personal information is seen as merely *using* that information and the transferring organization remains accountable for the information. As is further discussed, so long as the consent for the use of the information was broad enough to contemplate that the information would be processed in some capacity, then a *transfer* of information for those processing purposes requires no additional consent. Lastly, where this paper refers to *transfers* of personal information, reference is in fact being made to the concept of a *transfer for processing* as it is used in Principle 4.1.3. of the Schedule to PIPEDA.

the United States.

Much of the confusion stems from the mistaken *belief* that Canadian privacy laws require Canadian organizations to shield personal information from a foreign government's ability to lawfully access that information. Most countries, including Canada, have laws permitting government agencies to access personal information within their jurisdiction for national security and law enforcement purposes. Despite the fact that some of these laws potentially permit broader government access than the USA Patriot Act (such as in the United Kingdom), transfers that may be subject to the USA Patriot Act are the source of the most confusion and misinformation. This fact has been recognized by the Privacy Commissioner who has explained that it is consistent with laws in the United States, Canada and elsewhere to permit governments to seek information about individuals in connection with intelligence activities: "Governments around the globe have long exercised the right to obtain information held by organizations within their borders. Many Canadian laws also enable police, security agencies and government departments generally to obtain access to personal information held in Canada." The Commissioner noted that, in Canada, such information may be obtained under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*,<sup>7</sup> the *Department of Immigration and Citizenship Act*,<sup>8</sup> and the *Canadian Security Intelligence Service Act*.<sup>9 10</sup>

In this era of global data flows and automated processes, Canadian enterprises and government agencies, like their counterparts in other countries, face growing pressure to use information technology to contain costs and increase efficiency. Many of the leading suppliers of information technology are global companies, headquartered in the United States. The confusion within the marketplace about whether Canadian organizations can transfer their data to the United States for processing is having a negative impact on the ability of Canadian firms to conduct business with these American companies. As a result, Canadian firms that are under the erroneous impression that they must keep all personal information within Canada are forced to absorb higher operating costs.

A careful and thorough review of Canadian law, however, makes it clear that although organizations must meet certain conditions, Canadian privacy laws generally do not prohibit the international transborder flow of personal information from Canada to locations outside of Canada, including to the United States.

---

<sup>7</sup> S.C. 2000, c. 17

<sup>8</sup> S.C. 1994, c. 31

<sup>9</sup> R.S.C. 1985, c. C-23

<sup>10</sup> See *Transferring Personal Information about Canadians Across Borders* - Implications of the *USA PATRIOT Act*, Submission of the Office of the Privacy Commissioner of Canada to the Office of the Information and Privacy Commissioner for British Columbia, August 18, 2004. Online: [http://www.privcom.gc.ca/media/nr-c/2004/sub\\_usapa\\_040818\\_e.asp](http://www.privcom.gc.ca/media/nr-c/2004/sub_usapa_040818_e.asp)

## 1. CANADIAN FEDERAL LAW DOES NOT PROHIBIT THE CANADIAN PRIVATE SECTOR FROM TRANSFERRING PERSONAL INFORMATION TO THE UNITED STATES.

Almost all commercial activity in Canada is subject to some privacy regulation if that activity involves the collection, use or disclosure of personal information.<sup>11</sup> PIPEDA is the national law applicable to organizations that collect, use or disclose personal information in the course of commercial activity. PIPEDA does not apply if an organization's activity is covered by one of three<sup>12</sup> provincial private sector privacy schemes that have been deemed substantially similar to PIPEDA.

There is no language in PIPEDA to suggest that there is a prohibition on the transfer of personal information outside of Canada. In fact, the law explicitly contemplates transfers of personal information. Section 4.1.3 of the Schedule to the Act states that when transferring personal information, appropriate safeguards must be used so that the transferring organization remains accountable: "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." Importantly, and because the transferring organization remains accountable for the personal information involved in any transfer, there is no obligation in PIPEDA that is similar to that found in European data protection laws that restrict the international transfer of personal information only to those jurisdictions whose privacy laws have been declared "adequate" by some standard.

In those instances where the transfer of personal information outside of Canada has been examined, the Commissioner has found that the transborder flow was perfectly legal because all the necessary obligations imposed on the organization transferring the information were met. For example, in *PIPEDA Case Summary #333* (entitled "Canadian-based company shares customer personal information with U.S. parent"),<sup>13</sup> two individuals filed complaints concerning their security system provider. The complainants asserted that the company was using an inappropriate form of consent with respect to its practice of sharing customer personal information with its American parent company. Both complainants also expressed concern about the possibility of their

---

<sup>11</sup> A notable exception is that organizations operating in those provinces without private sector privacy legislation are not caught by any specific privacy legislation dealing with the handling of employment related personal information so long as the organization's activity is solely about managing the employment relationship (i.e., the organization has not taken its employees' personal information and sold it to, for example, a marketing firm. This type of activity would be caught by PIPEDA.).

<sup>12</sup> British Columbia, Alberta and Quebec.

<sup>13</sup> Online: [http://www.privcom.gc.ca/cf-dc/2006/333\\_20060511\\_e.asp](http://www.privcom.gc.ca/cf-dc/2006/333_20060511_e.asp)

personal information being accessed by United States government authorities as a result of the passage of the USA Patriot Act.

The Commissioner, however, determined that the company had taken the appropriate step of informing its customers about its personal information practices and was *not* required to obtain additional consent from its customers. Additionally, the organization properly safeguarded the information after it was transferred to the company in the United States because the American company was contractually bound to safeguard the personal information to the same extent as the Canadian company. In other words, the transferring organization remained accountable, the transfer was reasonable and the transfer was based on consent and adequate notice.

Thus, the statutory language in PIPEDA taken together with the Privacy Commissioner's interpretations of PIPEDA, clearly demonstrate that transfers outside of Canada are permitted. Of course, the transfer does not negate the overriding legal obligation to act reasonably and transparently in the collection, use and disclosure of personal information<sup>14 15</sup>).

## 2. CANADIAN FEDERAL LAW DOES NOT PROHIBIT CANADIAN FINANCIAL INSTITUTIONS FROM TRANSFERRING PERSONAL INFORMATION TO THE UNITED STATES.

The mistaken belief that Canadian privacy law prohibits the transfer of personal information to the United States is particularly wide-spread within the Canadian financial community. This belief is at odds with both the law and relevant government opinions on the matter. In the Statement of the Free Flow of Information and Trade in North America<sup>16</sup>, the Canadian and American, governments said: "Financial services, such as banking and insurance, are heavily dependent on data flows. When this activity takes place across national boundaries, it is important that countries work together to ensure differing regulatory regimes don't hinder cross-border data flows and international trade."

Neither PIPEDA nor sectoral banking laws prohibit the transfer of personal information to the United States or any other country.<sup>17</sup> While specific sectoral laws such as the *Bank*

---

<sup>14</sup> See, for example, section 5(3) of PIPEDA.

<sup>15</sup> See, for example, section 7 of PIPEDA.

<sup>16</sup> Mexico is also a signatory to the Statement. It was signed in February 2008 as part of the Security and Prosperity Partnership between Canada, the United States and Mexico. The Statement can be found at: <http://www.spp-psp.gc.ca/pdf/SPPStatement%20Free%20FlowFinal%20-%20eng-fre-spanish.pdf>

<sup>17</sup> Also potentially relevant would be the substantially similar private sector privacy laws in British Columbia, Alberta and Quebec. As is further elaborated, neither of these laws prohibits the transfer of personal information to the United States or any other country.

*Act*<sup>18</sup> and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*<sup>19</sup> do create various reporting obligations on specific organizations, none of these laws contain any language that restrict an organization's ability to transfer personal information outside of Canada, including to the United States.

The financial sector's ability to transfer personal information has been specifically examined by the Privacy Commissioner. In each instance, the Commissioner concluded that Canadian law allows the transfer of personal information to other countries. Importantly, as elaborated below, one of the paramount conclusions in these cases is the finding that the transfer be based on a clear notice that a transfer outside of Canada may take place. If such a notice describing that personal information may be transferred outside of Canada is in place on the consent form or privacy policy, no further consent is required. The organization is not required to go back to each individual customer to obtain additional consent permitting the transfer of their personal information outside of Canada.

Thus, in *PIPEDA Case Summary #313* (entitled: *Bank's notification to customers triggers PATRIOT Act concerns* and often referred to as the "CIBC VISA case"),<sup>20</sup> the issue of the American government's ability to obtain personal information once it is transferred outside of Canada was precisely at issue. It was argued by the complainants that making the information vulnerable to a foreign government's ability to seize it was unreasonable. In this matter, a bank issued a notice to its customers that it was outsourcing a function required for the processing of credit card accounts and that the company which was to perform the processing was located in the United States. Clearly there was personal information of a financial nature being transferred to the United States.

After reviewing the contract between the bank and the third party, and after noting the various clauses concerning the proper safeguarding of the personal information, the Commissioner concluded that PIPEDA *cannot* "force Canadian companies to stop outsourcing to foreign-based service providers". Instead, PIPEDA requires Canadian organizations to be transparent about their personal information handling practices and to remain accountable by protecting customer personal information in the hands of foreign-based third-party service providers through the use of contractual clauses.

On the issue of whether or not the transfer of personal information to the United States was an activity that required the organization to obtain additional consent, the Commissioner was clear that consent is *not* required for the transfer of personal information outside of the country, including to the United States. In her finding, she stated:

---

<sup>18</sup> S.C. 1991, c. 46.

<sup>19</sup> S.C. 2000, c. 17.

<sup>20</sup> Online: ([http://www.privcom.gc.ca/cf-dc/2005/313\\_20051019\\_e.asp](http://www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp))

This Office has taken the position that companies are not required to provide customers with the choice of opting-out where the third-party service provider is offering services directly related to the primary purposes for which the personal information was collected. *A customer provides consent to the primary uses of personal information when he or she initially signs the application form or when he or she continues to use the service after being advised of substantive changes to the service agreement.*<sup>21</sup> [emphasis added]

Therefore, in any transfer of personal information outside of Canada, a Canadian organization can rely on the initial consent they receive from their customers and process the personal information outside of Canada without further consent so long as the following conditions are met: (i) adequate notice is provided to the customers that their personal information may be transferred outside of Canada; and (ii) the processing of the personal information is directly related to the purpose for which the organization initially collected it. In coming to this conclusion, the Commissioner ensured that the organization had a valid business reason to transfer the personal information outside of Canada.

Similarly, in the Swift case,<sup>22</sup> the Canadian Privacy Commissioner also affirmed the right of financial services institutions to store personal information outside of Canada. In its opinion on this case, the Commissioner stated:

As part of SWIFT's business operations, it backs up all of its data on several databases, one of which is in the United States. *Generally, the Act does not prohibit an organization that operates in Canada from storing that information outside the country if it otherwise abides by the Act's requirements.* Based on the submissions and evidence provided by SWIFT, it is clear that maintaining the backup databases outside of Canada achieves legitimate business

---

<sup>21</sup> *PIPEDA Case Summary #313* (entitled: *Bank's notification to customers triggers PATRIOT Act concerns*). Online: [http://www.privcom.gc.ca/cf-dc/2005/313\\_20051019\\_e.asp](http://www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp).

<sup>22</sup> *Report of Findings, April 2, 2007*. Online: [http://www.privcom.gc.ca/cf-dc/2007/swift\\_rep\\_070402\\_e.asp](http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_e.asp). Note that SWIFT (Society for Worldwide Interbank Financial Telecommunication) supplies messaging services and software to over 7,900 financial institutions in more than 200 countries. The messages are usually used for cross-border payments, securities clearing and settlement, and treasury and trade services. Some messages contain personal information, such as name, address, account number, amount of transfer. All were stored on databases that are mirrored in both Europe and the United States. Following 9/11, the United States began issuing subpoenas to SWIFT for certain data held in SWIFT's United States-based operating centre. SWIFT confirmed that personal information originating from or transferred to Canadian financial institutions was likely included in data handed over to the United States.

needs. [emphasis added]

Moreover, in the companion case to the SWIFT case, the Privacy Commissioner examined the role played by the Canadian banks in the transfer of personal information to an organization that processed the information outside of Canada.<sup>23</sup> The banks' notification to customers about their practices with respect to processing personal information outside of Canada was considered adequate, thus confirming that there was no need for the bank to obtain further consent from its customers to cover the transfer outside of Canada. In this regard, all of the banks' privacy policies (both in electronic and paper format) contained notification to customers that they used third-party processors, some of which may have been located outside of Canada. While differing slightly from bank to bank, each notice basically indicated that while customer information was outside of Canada, it was subject to the laws of that country.

To summarize, the issue of transferring personal information outside of Canada, including to the United States, has been carefully examined by the Canadian Privacy Commissioner, including specific instances arising within the financial sector. The Commissioner's conclusion is clear: financial institutions may transfer personal information outside of Canada without obtaining the customers' additional consent for such transfers so long as the financial institution provides notice to customers about its information practices and remains accountable for safeguarding the information.

### 3. CANADIAN LAW DOES NOT PROHIBIT THE FEDERAL GOVERNMENT FROM TRANSFERRING PERSONAL INFORMATION TO THE UNITED STATES.

The Canadian *Privacy Act*, which is the public sector law that applies to the federal government, does not restrict the processing of personal information by a third party located outside of Canada. The Treasury Board of Canada<sup>24</sup> has issued a policy requiring that each federal government institution establish measures to ensure that the government institution meets the requirements of the *Privacy Act* when contracting with private sector organizations, or when establishing agreements or arrangements with public sector organizations.<sup>25</sup> The policy's sole reference to the transborder flow of personal information requires only that government institutions [ensure] that appropriate privacy protection clauses are included in contracts or agreements that may involve

---

<sup>23</sup> *PIPEDA Case Summary #365* (entitled "Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered"). Online: [http://www.privcom.gc.ca/cf-dc/2007/365\\_20070402\\_e.asp](http://www.privcom.gc.ca/cf-dc/2007/365_20070402_e.asp)

<sup>24</sup> The government institution responsible for implementing government-wide policy.

<sup>25</sup> Section 6.2.10 of the Treasury Board Policy on Privacy Protection. Online: [http://www.tbs-sct.gc.ca/pubs\\_pol/gospubs/TBM\\_128/CHAP1\\_1-2\\_e.asp](http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP1_1-2_e.asp)

intergovernmental or transborder flows of personal information.<sup>26</sup>

The Treasury Board's policy statement stems from a 2004 study and subsequent report entitled: *Report on Assessment of Privacy Concerns Related to USA PATRIOT Act*.<sup>27</sup> Part of that Report included a guidance document relating to the contractual process. A general theme of these documents is an acknowledgement that the transborder flow of personal information is permitted. To ensure the proper administration of the transborder flow, government guidance suggests that government institutions wishing to outsource functions involving the transfer of personal information ensure that adequate safeguards be put into place using contractual clauses with the service provider. The safeguards may include ensuring that :

- the government institution has a right to audit and inspect the service provider;
- the service provider segregate the data;
- the service provider agree to provide data breach notification;
- the service provider agree to restrict access to the data;
- the service provider agree that the government institution retains control over the information and may obtain the records upon request;

the service provider agree that it may not disclose the information under any circumstances not provided in the contract; and

- the service provider agree not to use sub-contractors without prior notice and approval from the government institution.<sup>28</sup>

None of these provisions contains any language requiring the service provider to keep personal information inside Canada.

The Privacy Commissioner played a role in the development of the Treasury Board Guidance. At the time, she recognized the importance of the government's ability to continue to outsource. She said:

Just last month, Canada's Treasury Board Secretariat published a strategy to address concerns about the USA PATRIOT Act and transborder data flows. My Office was consulted on the development of this policy. A Risk analysis must identify and suggest how to mitigate the

---

<sup>26</sup> Section 6.2.11 of the Treasury Board Policy on Privacy Protection. Online: < [http://www.tbs-sct.gc.ca/pubs\\_pol/gospubs/TBM\\_128/CHAP1\\_1-2\\_e.asp](http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP1_1-2_e.asp)>

<sup>27</sup> Online: [http://www.tbs-sct.gc.ca/pubs\\_pol/gospubs/TBM\\_128/usapa/introduction\\_e.asp](http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/usapa/introduction_e.asp)

<sup>28</sup> Online: [http://www.tbs-sct.gc.ca/pubs\\_pol/gospubs/TBM\\_128/usapa/introduction\\_e.asp](http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/usapa/introduction_e.asp)

various privacy threats. Encryption, privacy impact assessments, firewalls and strong contractual language will go far in all but the most sensitive cases. *This tailored approach, rather than an outright ban on outsourcing of personal information, seems to me to provide a practical and workable way of dealing with privacy protection issues.*<sup>29</sup>[emphasis added]

#### 4. EXCEPT IN CERTAIN SITUATIONS IN BRITISH COLUMBIA AND NOVA SCOTIA, CANADIAN PROVINCIAL LAWS DO NOT PROHIBIT THE TRANSFER OF PERSONAL INFORMATION TO THE UNITED STATES.

The principles enunciated from the federal jurisdiction also apply to the provinces, and neither the private sector nor the public sector legislation in the provinces prohibits the transfer of personal information outside of Canada, including to the United States, subject to two exceptions.

Those two exceptions are British Columbia and Nova Scotia. However, even in those provinces, the restrictions are only with respect to the laws applicable to public bodies, are not categorical and provide for several exceptions. For example, the restrictions do not prevent an American organization from *accessing* personal information kept within British Columbia or Nova Scotia so long as the information remains in Canada. This means that an American service provider may perform work for a public body in these provinces if the service provider's access to personal information is incidental to the service provided. While the *transfer* of personal information outside of Canada may be circumscribed, providing a non-Canadian service provider incidental *access* to personal information is permitted.

A separate regime exists in Quebec. There the law requires provincial government bodies and private sector entities to ensure that personal information receives protection equivalent to that afforded under the province's privacy laws before it is released outside the province or entrusted to an organization located outside Quebec to hold, use or release it. If the public body or private sector entity considers that the information will not receive equivalent privacy protection, it must refuse to release the information or refuse to entrust the organization with the task of holding, using or releasing it on its behalf. This provision has never been held to mean that the law restricts the flow of information to the United States.

The remaining provinces' privacy laws do not prohibit the transfer of personal

---

<sup>29</sup> Privacy Commissioner's speech delivered May 5, 2006 entitled: *A Canadian Perspective on Data Protection - Data Protection and Security: A Transnational Discussion*. Online: [http://www.privcom.gc.ca/speech/2006/sp-d\\_060505\\_e.asp](http://www.privcom.gc.ca/speech/2006/sp-d_060505_e.asp)

information outside of Canada, including to the United States, though some provinces, such as Alberta, have some guidance or policy documentation similar to the federal Treasury Board guidelines referred to above.<sup>30</sup>

## CONCLUSION

Despite repeated assurance from the Canadian government that personal information may be transferred outside Canada, the mistaken perception that Canadian law somehow prohibits the transfer of personal data to the United States persists. As outlined above, however, Canada's privacy laws recognize the importance of transborder data flows and permits them, with few exceptions. In doing so, they also attach significant importance to the protection of personal information. As a result, Canadian business and government organizations are free to engage in commercial relationships that involve the processing of information in the United States as long as doing so is reasonable and as long as they are transparent, provide notice, and ensure that adequate safeguards are in place.

In further support of these concepts, both governments, in their Statement of the Free Flow of Information and Trade in North America noted that

International trade depends on seamless and uninterrupted information flows across companies, jurisdictions and borders. Networks function as conduits, channeling business information, processing data to carry out business processes and operations. The Internet has revolutionized advanced production and distribution activities, creating global supply chains that operate across virtually all sectors of the economy. It has digitized economic activity. Further, global sourcing of business processes has become an invaluable tool for improving corporate productivity and efficiency and achieving economic gain in many economic sectors, thus enhancing competitiveness for North America.

Cross-border data flows are an important underpinning of all international trade transactions<sup>31</sup>

In this paper we have clarified that these cross-border data flows -- which benefit

---

<sup>30</sup> See, for example, the Alberta Privacy Commissioner's document concerning transborder data flows in the public sector entitled "Public Sector Outsourcing and Risks to Privacy Report". It can be found at: <http://www.oipc.ab.ca/foip/detailspage.cfm?id=2502>

<sup>31</sup> Mexico is also a signatory to the Statement. It was signed in February 2008 as part of the Security and Prosperity Partnership between Canada, the United States and Mexico. The Statement can be found at: <http://www.spp-psp.gc.ca/pdf/SPPStatement%20Free%20FlowFinal%20-%20eng-fre-spanish.pdf>

companies on both sides of the border, further trade and provide growth opportunities -- are permissible under Canadian law. The transfers are subject to reasonable controls and contractual requirements as outlined above, but there is no outright prohibition. It is only in certain defined circumstances involving public information and public institutions in British Columbia and Nova Scotia where there are some restrictions on transferring (but not outright prohibition on accessing) such information outside of Canada.