PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DEFENSE DE L'INTERET PUBLIC
ONE Nicholas Street, Suite 1204, Ottawa, Ontario, Canada K1N 7B7
Tel: (613) 562-4002. Fax: (613) 562-0007. e-mail: piac@piac.ca. http://www.piac.ca

April 15, 2010

VIA E-Mail ONLY

Melanie Millar-Chapman
Office of the Privacy Commissioner of Canada
112 Kent Street
Place de Ville, Tower B, 3rd Floor
Ottawa, ON
K1A 1H3

Dear Ms. Millar-Chapman:

Re: 2010 Consumer Privacy Consultations – Comments of PIAC

The Public Interest Advocacy Centre (PIAC) is pleased to enclose their comments on the privacy implications of cloud computing for the 2010 Consumer Privacy Consultations of the Office of the Privacy Commissioner of Canada.

As well, PIAC is interested in participating in panel discussions for the consultation and we look forward to hearing from the OPCC in this regard.

Thank you.

Yours truly,

John Lawford
Counsel

Janet Lo
Counsel

encls.

2010 Consumer Privacy Consultations

Privacy Implications of Cloud Computing

Comments of the Public Interest Advocacy Centre

April 15, 2010

John Lawford, Counsel
(613) 562-4002 x 25
lawford@piac.ca

Janet Lo, Counsel
(613) 562-4002 x 24
jlo@piac.ca

Public Interest Advocacy Centre
ONE Nicholas Street, Suite 1204
Ottawa, Ontario K1N 7B7

About the Public Interest Advocacy Centre

The Public Interest Advocacy Centre (PIAC) seeks to advance the interests of individuals and groups who are generally unrepresented or underrepresented in issues of major public concern. We champion those issues that involve the delivery of important public and utility services. The Centre seeks to ensure that the public interest is served, and not neglected, by decision makers in government and the private sector when decisions are made about consumer issues. The Centre undertakes solid legal and research services on behalf of consumers. The Centre focuses primarily on consumer issues concerning telecommunications, energy, privacy, the information highway, electronic commerce, financial services, broadcasting, and competition law.

Jurisdiction and transfer issues

The jurisdictional and outsourcing aspects of cloud computing pose the greatest risks for consumers. A company processing[1] its customer's personal information on servers in Canada does not run into jurisdictional or outsourcing complexities. Once the company processes the information outside of Canada or outsources the processing of data to third parties, the protection of customers' privacy may become frustrated.

PIAC submits that for the most part, consumers are unaware that their personal information may be processed on servers in different countries with different state laws applicable. In general, *PIPEDA* Principle 1 states that an organization is responsible for the personal information under its control. At the same time, PIPEDA section 7(3) leaves an opening for a company to disclose personal information without the individual's knowledge or consent if ordered to by a foreign court having the competent jurisdiction to compel its production. As a result, for instance, an activist opposed to a country's government may object to his orher personal information being processed on servers in that country. Along the same line, a political refugee may object to his or her personal information being processed in the country from which he or she fled. Others may simply choose not to have their personal information processed on servers in the United States, where the *USA PATRIOT Act* is in effect. All companies that process their Canadian customers' personal information on servers outside of Canada should at the very least inform their customers which jurisdictions their data may be processed and offer an opportunity to opt-out, consistent with the principles of notice and consent

An issue linked to jurisdiction is outsourcing. Companies often use third parties for data processing, subjecting their customers' personal information to the third parties' security and privacy policies without their customers' knowledge of them. Moreover, the third parties may be located in different jurisdictions. Under *PIPEDA* Principle 4.1.3, a company that transfers personal information to a third party for processing remains responsible for the information and must use contractual or other means to ensure a comparable level of protection. Principle 4.8 requires that companies be open and

[1] In this letter, "processing" is taken to cover storage as well, so as to encompass the collection, use and disclosure of data.

transparent about the manner in which they handle their customers' personal information.

There have been a number of OPC findings applying Principle 4.1.3 and Principle 4.8 to the transfer of personal information by companies, (e.g. CIBC,[2] SWIFT[3] and Canada.com[4]) so that as long as the companies outsource to other companies with comparable security and privacy policies, and show transparency by advising their customers of such, the transfer of data would be permissible.

In the case of CIBC, subsection 245(1) of the *Bank Act* required the bank to apply for and receive approval of the Office of the Superintendent of Financial Institutions (OSFI) in order to have its customer account records processed outside of Canada. OSFI guidelines require that the bank "pay particular attention to the legal requirements of that jurisdiction, as well as the potential foreign political, economic and social conditions, and events that may conspire to reduce the foreign service provider's ability to provide the service, as well as any additional risk factors that may require adjustment to the risk management program."[5] In the OPC's *Guidelines for Processing Personal Data Across Borders*, it is stated that the OSFI guidelines set a high standard for the protection of sensitive financial information by financial institutions, implying that when personal information is less sensitive, the standard for the protection of the information with a comparable level of protection need not be as stringent. In PIAC's previous letter to the OPC concerning online tracking, profiling and targeting, there are definitional issues as to what information is defined as "sensitive" personal information. PIAC submits that all personal information relating to a Canadian consumer that is processed by a third party outside Canada, whether sensitive or not, ought to be protected contractually through the same guidelines as those provided by the OSFI. The reason for this stems from the nature of "cloud computing", which by definition involves the management and storing of massive amounts of interlinked data. As more and more information about an individual is stored in the cloud, the distinction between sensitive and non-sensitive data begins to dissolve. Therefore, a global amendment to *PIPEDA* that incorporates OSFI guidelines relating to transfer of data is the best way to protect all personal information processed in the cloud.

Furthermore, in *Lawson v. Accusearch*,[6] the Federal Court of Canada found that *PIPEDA* extended to foreign entities that receive and transmit communications to and from Canada, and that collect information about individuals in Canada. In the case of SWIFT, the Commissioner found that there was a real and substantial link between the Belgian company (to whom Canadian banks outsourced the processing of customer financial data) and Canada. Since *PIPEDA* was applicable to SWIFT, the Commissioner concluded that paragraph 7(3)(c) allowed the company to disclose information to U.S. authorities. PIAC recognizes that PIPEDA cannot serve to supplant the foreign laws applicable to foreign third parties that process personal information about Canadian

[2] PIPEDA Case Summary #2005-313.
[3] PIPEDA Case Summary #2007-365.
[4] PIPEDA Case Summary #2008-394.
[5] *Supra* note 4.
[6] *Lawson v. Accusearch Inc.*, 2007 FC 125 (CanLII).

individuals, as stated in the CIBC case. Notwithstanding the foregoing, it would be desirable that the contractual means used to ensure a comparable level of protection of personal information processed by third parties outside of Canada, consistent with Principle 4.1.3, include provisions stipulating that the third party shall comply with *PIPEDA* and submit to Canadian jurisdiction. Adding this requirement would provide another layer of protection for the personal information of Canadian consumers. Any difficulties implementing such a requirement are perhaps representative of a greater deficiency of the organization-by-organization approach that Canada has taken, in contrast to the higher-level diplomatic approach taken by the European Union. The EU, concerned about personal information processed in the United States, established the U.S. Safe Harbor Privacy Principles[7] in conjunction with the U.S. government. This top-down approach, in which foreign third party providers have the incentive of legal compliance when dealing with companies that transfer personal information of Canadian consumers, may be more effective in addressing risks associated with outsourcing the processing of personal information before-the-fact.

Regarding the nature of notification to consumers about the handling of their personal information, Principle 4.8 of Schedule 1 requires the company to be open and transparent about the way it handles its customers' personal information. In the case of CIBC, the bank had informed its clients that their personal information may be processed in the United States and hence that U.S. authorities may be able to obtain disclosure of the information under the laws of the country. This notice satisfied the Commissioner that the bank carried out its obligation under Principle 4.8.

However, some companies are vague with respect to jurisdiction in their privacy policies. For example, Google's privacy policy states the following:

> "Google processes personal information on our servers in the United States of America *and in other countries*. In some cases, we process personal information on a server *outside your own country*."[8] [Emphasis added]

Microsoft's privacy policy[9] is similarly vague. As it stands now, Principle 4.8 leaves consumers powerless when confronted with either vague terms of service relating to the processing of their personal information or a change to existing terms of service specifying a new country (or third party) where the processing of their information will be transferred to. Since it is both theoretically and technically possible for companies to delimit (or at least specify) where their customers' personal information will be processed, the OPC's position that "at the very least, a company in Canada that outsources information processing to the United States should notify its customers that the information may be available to the U.S. government or its agencies under a lawful order made in that country"[10] must be extended to include the right for Canadian consumers to know precisely which countries their personal information might be

[7] http://www.export.gov/safeharbor/eg_main_018236.asp
[8] http://www.google.com/privacypolicy.html
[9] http://privacy.microsoft.com/en-ca/fullnotice.mspx
[10] http://www.priv.gc.ca/cf-dc/2005/313_20051019_e.cfm

processed in and be offered (perhaps through a minimum notice period in case the consumer is already a customer) a reasonable opportunity to object and/or cancel their service with the company. After all, in contrast to the case of CIBC, the country in which an individual's personal information is being processed in may have national security legislation even more invasive than the *USA PATRIOT Act*, which, in the context of "comparable protection", the Commissioner noted[11] is somewhat similar to Canada's own. Of note is that Mimecast, an email management service provider based in the United Kingdom and catering to law firms and banks among other businesses, offers its clients the option of having its service deployed, managed and supported for them in a particular jurisdiction.[12]

Security and integrity of the data

Security is paramount when dealing with consumer data stored in the cloud, especially since the data is tied to the consumer. A typical argument put forth by proponents of the cloud computing model is that data stored on servers connected to the cloud are at least as secure as consumers computers at home (assuming the latter are also connected to the Internet). This argument has some merit, at least *prima facie*, since it is probably true that cloud computing servers employ greater security measures than the average home computer. However, once enough data deemed valuable to potential hackers or intruders is stored on one server (or network of servers), they may concentrate their efforts more easily.

Though security breaches of servers is not a novel phenomenon, recent attacks by adaptive and savvy hackers are cause for alarm. On April 6, 2010, Canadian researchers exposed an online spy ring, originating in China, that compromised computers systems in the Dalai Lama's offices, Indian government, business and academic institutions and the United Nations, to name a few.[13] The data collected by the hackers contained sensitive data from 16 countries, including visa applications of Canadian citizens.[14] In their report on the matter, entitled *Shadows in the Cloud: Investigating Cyber Espionage 2.0*[15], the researchers explain that contributing factors to the dangerous ecosystem of crime and espionage on the Internet are the advancements in technology coupled with poor security practices:

> "Attackers employ complex, adaptive attack techniques that demonstrate high-level ingenuity and opportunism. They take advantage of the cracks and fissures that open up in the fast-paced transformations of our technological world. *Every new software program, social networking site, cloud computing, or cheap hosting service that is launched into our*

[11] *Supra*, note 4.
[12] http://www.mimecast.com/small-business/mimecast-off-shore/
[13] http://www.theglobeandmail.com/news/technology/canadian-researchers-reveal-online-spy-ring-based-in-china/article1524228/
[14] *Ibid.*
[15] Ron Deibert and Rafal Rohozinsky, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, April 6th, 2010. The report may be accessed at http://www.shadows-in-the-cloud.net

everyday digital lives creates an opportunity for this ecosystem to morph, adapt, and exploit.

It has also emerged because of poor security practices of users, from individuals to large organizations. We take for granted that the information and communications revolution is a relatively new phenomenon, still very much in the midst of unceasing epochal change. Public institutions have adopted these new technologies faster than procedures and rules have been created to deal with the radical transparency and accompanying vulnerabilities they introduce."[16] [Emphasis added]

The researchers mentioned that the infrastructure created by the hackers to access the computer systems involved utilized "freely available social media systems that include Twitter, Google Groups, Blogspot, Baidu Blogs, blog.com and Yahoo! Mail."[17] Thus, it is apparent that popular cloud-based services serve as tempting and focused intermediaries for adaptive hackers. As personal data becomes more and more valuable to advertising companies,[18] security measures become increasingly important safeguards of privacy. Due to the potential for intrusion and other security risks such as human error, there is a need for a very high standard of data security when personal information is stored on servers. Data encryption, a technological measure mentioned under *PIPEDA* Principle 4.7.3, is but one of many methods of securing data and one that should be employed by all cloud computing companies. Currently, there exist standards for information storage security such as ISO 27001[19], which provides a comprehensive standard for a company's information security management system. Since Canadian consumers would clearly benefit from knowing that their personal data is stored with companies that implement a sufficient and known level of security, an independent or governmental body may be appointed to create and enforce such a standard.

Finally, the lack of a federal mandatory data breach notification policy puts Canadian consumers at risk should a company not inform its customers of a data breach. PIAC recommends that the OPC's voluntary guidelines on data breach notification be reviewed and made mandatory under PIPEDA.

Data retention

Currently under *PIPEDA* Principles 4.5.2 and 4.5.3, organizations are recommended to develop guidelines and implement procedures regarding retention of personal information, including minimum and maximum retention periods. Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased or anonymized. Some companies do address the issues of data retention in their privacy

[16] *Ibid.* at p.i.
[17] *Ibid.* at p.iv.
[18] A recent complaint to the FTC alleges that real-time data of individuals are being bought and sold through ad auctions and exchanges. The complaint may be accessed at http://www.democraticmedia.org/files/u1/20100407-FTCfiling.pdf
[19] http://www.iso.org/iso/catalogue_detail?csnumber=42103

policies (e.g. Google Docs[20]) and others do not (e.g. Microsoft Office Live[21]). Canadian consumers must be able to have faith that once they delete their personal information from the cloud, such data may only persist on servers within the stipulated minimum and maximum retention periods.

Copyright considerations

Jumping on the cloud computing bandwagon are telecom companies who attempted to market or are marketing "network-based PVRs", which allow their subscribers to record and store content in the cloud, and dispense with the expensive hardware that regular personal video recorders come equipped with. While some telecom companies, including Bell, have touted the benefits of network-based PVRs, it appears that such devices would be prohibited under the time-shifting provision of *Bill C-61*[22]. Consumers buying devices such as these could face serious copyright infringement liability should the *Bill* come into force. Professor Michael Geist argued that "the recent revelations about Bell's PVR raises the question about the corporate responsibility of companies that are effectively downloading legal risk onto their customers by marketing products that could raise the prospect of liability."[23] PIAC is of the view that telecom companies ought to inform potential customers of their products of any potential liability that may be attached to the use of the products.

Lawful access

PIAC shares the concern raised by the OPC in "Reaching for the Cloud(s): Privacy Issues related to Cloud Computing" that in the situation "where many companies are using a centralized cloud infrastructure, a lawful access request to the cloud provider has the potential to garner information from all the diverse companies."[24] As such, there is a risk that data subject to a search warrant, for example, could be connected in the cloud to other personal data not subject to the warrant, essentially providing access to personal information that would not otherwise be available to authorities.

Cloud computing further exacerbates the problems with present PIPEDA subss. 7(3)(c.1) and 7(3)(d), which permit companies on request by a "government institution" or even on the business's own initiative to send information to government authorities without a warrant due to mere suspicion it is connected to a criminal offence or impacts the security of the Canadian state. Cloud computing solicits, creates and stores so much more information than previously (now, up to and including an entire workflow and harddrive of a person) was stored on a home computer (a search of which still requires a warrant) that these PIPEDA exemptions now look positively monstrous, in the sense of being a method of circumventing judicial approval of search and seizure, privacy requirements and even the rule of law. We see a clear conflict of the present warrant

[20] http://www.google.com/google-d-s/privacy.html
[21] http://privacy.microsoft.com/en-ca/officelive.mspx to be read in conjunction with http://privacy.microsoft.com/en-ca/fullnotice.mspx
[22] *Bill C-61*, 39th Parliament - 2nd Session, s.29.23.
[23] http://www.thestar.com/sciencetech/technology/article/480217
[24] http://www.priv.gc.ca/information/pub/cc_201003_e.cfm

requirements for home computer searches and a "virtualization" of that home computer "in the cloud" subject to delivery to government authorities at any time by private parties on mere suspicion. Cloud computing makes the argument for repeal of these provisions all the more urgent.

Secondly, in relation to proposed "lawful access" legislation in particular, *Bill C-46*[25] in its present form, which adds new investigative powers in relation to computer crime and the use of technologies in the commission of crimes, amends s.487.012 of the Criminal Code of Canada to allow a justice or judge to order a person to preserve "computer data" in their possession or control. Under s.15 of the proposed Bill, s.487.012(2) is amended to require that Form 5.002 be submitted under oath to the justice or judge before the order is made. Form 5.002 includes the following text: "The informant therefore requests that (name of the person) be ordered to preserve (specify the computer data) that is in their possession or control when they receive the order for 90 days after the day on which the order is made." "Computer data" under s.342.1(2) is re-defined in s.11(4) of the Bill as "representations, including signs, signals or symbols, that are in a form suitable for processing in a computer system." There appears to be no legislative or regulatory limit on the scope of "the computer data", which may then be broad enough to encompass personal information of other people than those whose data is the object of the order and which happens to be connected the data sought by the authorities. As a result, PIAC is concerned that unless a judge or justice of the peace is astute enough to require a detailed description of the exact "computer data" sought, that a data "dump" of a customer's information holdings would automatically occur – leaving open the real possibility that this could be a "fishing expedition" tool and law enforcement would obtain evidence of potential crimes that the warrant in question was not issued in aid of investigating.

Function creep

With a large bank of statistics and data, there also exists an allure for cloud-based service providers to profit from the dataset in ways that would otherwise not be available to them with the traditional PC-based software model. The progress and growth in the area of behavioural-targeted advertising is testament to the fact that personal data is valuable to advertising companies.[26] Because of this, cloud-based service providers companies would likely be tempted to broaden their consents.

While the privacy risks of behavioural targeting are being dealt with in the context of the OPC's consultation on online tracking, profiling and targeting, PIAC feels that such risks are exacerbated by the cloud computing model when selling or sharing data becomes profitable to those companies. Specifically, there must be a clear threshold between acceptable advertising practices that support the cloud-based model and practices deemed too intrusive. Moreover, the more personal information is collected, the greater the effect of the security risks associated with it.

[25] *Bill C-46*, 40th Parliament - 2nd Session.
[26] Please see PIAC's letter to the Office of the Privacy Commissioner dated March 15th, 2010.

Control of customer data

The controversy surrounding Amazon's decision to delete e-books on its Kindle handhelds that were purchased by customers highlights a general lack of control that consumers have on their data stored in the cloud. In that case, the New York Times reported that when Amazon realized that it had sold its customers digital copies of George Orwell's "Animal Farm" to which it did not have the rights to, the company deleted the digital copies from its customers' handhelds and refunded them.[27]

This lack of control over consumer data extends to personal information stored by cloud-based service providers as well.

Compromised meaningful choice and consent

As a growing dependence on the cloud computing model arises among consumers, PC-based software content may begin to dwindle. For instance, the allure of being able to organize and edit photos for free online, with the added benefit of being able to share them online with friends and family, may obviate the need for similar software content sold on disc. Should the free, advertising-supported model become the most viable model for software developers and replace the traditional model, meaningful choice and consent to the former model would be compromised.

Conclusion

PIAC is grateful for this opportunity to comment on cloud computing. We look forward to working with the Office of the Privacy Commissioner on this important consumer issue.

[27] http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html