2010 Consumer Privacy Consultations:

What Lies Behind the Lifting Cloud?

David Fewer, Director
Chigbo Ikejani, Student Intern
Alicia Kim, Student Intern

April 15, 2010

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)
Centre for Law, Technology and Society
University of Ottawa – Faculty of Law, Common Law Section
57 Louis Pasteur Street, ON., K1N 6N5
Tel: (613) 562-5800 ext. 2553
Fax: (613) 563-5417
www.cippic.ca

Table of Contents

Part I Background 1
A. The Nature and Advantages of Cloud Computing 1
(a) Cost Containment, Immediacy and Scalability 2
(b) Reliability and Efficiency 2
Part II Cloud Computing and Privacy – PIPEDA's Implications 3
A. Outsourcing and Cross-Boundary Issues 3
(a) PIPEDA 3
(b) Privacy Concerns in Cloud Computing 3
(c) Canadian Approaches to Outsourcing Canadians' Personal Information 4
(d) PIPEDA Reforms 5
B. Use and Disclosure 6
(a) PIPEDA 6
(b) Privacy Concerns in Cloud Computing 6
(c) Canadian Approaches to Use and Disclosure of Personal Information 7
(d) PIPEDA Compliance 8
C. Data Retention 8
D. Data Security and Technical Safeguards 9
Part III Conclusion 10

Part I Background

Internet use has changed multiple times. The last decade saw the emergence of "Cloud Computing" – a phenomenon characterized as an "unstoppable force."[1] Cloud Computing refers to the provision of Internet-based services that has the effect of moving computing and data away from local desktop and portable PCs and into distant computing resources. While it is the abstraction between the physical infrastructure and the owner of the information that the attraction of Cloud Computing lies, it is also this abstraction that creates particular concerns relating to privacy and personal information. The purpose of this submission is to address these concerns and to assess the limitations and effectiveness of PIPEDA balancing Canadians' interests in privacy protection with optimized and efficient utility of computing.

CIPPIC's view is that, as with social networking, behavioural targeting, deep packet inspection, and other potentially invasive emerging Internet-based services and technologies, privacy laws facilitate – not frustrate – the deployment of these technologies. But this facilitation directs the roll-out of these technologies and services in particular ways that are consistent with Canadians' privacy interests. As our analysis of Cloud Computing will demonstrate, these services and technologies do and will continue to challenge Canadians' privacy interests. The key to successful deployment of Cloud Computing services and technologies is to accommodate privacy interests through transparent practices, by offering Canadians choice and control over the manner in which their personal information is collected, used and disclosed (including liberal use of "opt-in" mechanisms where warranted), and avoiding unexpected and unreasonable practices.

A. The Nature and Advantages of Cloud Computing

Cloud Computing represents a major change in how we store information and run applications. Traditionally, we have hosted applications and stored data locally, on our own desktop computer or on a local server. Cloud Computing, in contrast, allows one to work and collaborate through the Internet through remote central servers. Individuals and businesses may use applications and store data on a web-based virtual platform rather than on their own computers.[2] This assemblage of "remote central servers" and "web-based virtual platforms" are referred to as the "cloud".[3] The term "cloud" is used as a metaphor to depict the underlying infrastructure it represents as an abstraction.[4]

For many software users, especially IT businesses, Cloud Computing promises optimistic changes to traditional IT business models to accommodate ever – increasing IT demands.[5] The promise of Cloud Computing is arguably revolutionizing the IT services world by transforming computing into a ubiquitous utility with attributes such as cost savings, immediacy, scalability, efficiency and reliability.

---

[1] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," <http://www.educause.edu/Resources/SecurityGuidanceforCriticalAre/196517>, where it is stated that Cloud Computing is becoming a global connector of the world's information with its attractive potential to afford users with operating and economic efficiencies of computing.

[2] David A. Couillard, "Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectation in Cloud Computing" (2009) 93 Minn. L. Rev. 1943 at 2205.

[3] Michael Miller, "Cloud Computing Pros and Cons for End Users," <http://www.informit.com/articles/article.aspx?p=1324280> [Miller].

[4] Simon Hodgett, "Cloud Computing Raises Privacy Concerns," *The Lawyers Weekly*, 28:37, (13, February 2009).

[5] Eric Knorr, "What Cloud Computing Really Means," *Infoworld*, <http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031>.

(a) Cost Containment, Immediacy and Scalability

Cloud-based applications are cheaper for businesses because services and storage are made available easily on demand by a third party provider. Businesses do not have to locally install capital intensive servers and purchase local infrastructure as cloud-based applications run in the cloud.[6] Similarly, there is no need for individuals to purchase expensive software applications because their information is saved not on their desktop PC, but in a Cloud Computing system.[7] Also, the cloud is often priced as a pay as you go service, or even free in the case of some applications and services.[8] At the same time, Cloud Computing offers effectively unlimited storage capacity. And because users pay a provider only for what they use, it allows them to save on wasted resources, such as unused server space, and contain costs in terms of existing technology requirements and experiments with new technologies and services without a large investment.[9] The cloud also reduces costs associated with time delays because it can be set up in a single day.[10] In addition, Cloud Computing is a cost effective scalability solution for businesses because the cloud offers virtually unlimited storage on demand, offering increased flexibility for evolving IT needs.[11]

(b) Reliability and Efficiency

Cloud computing allows businesses to focus their efforts to innovation and productive development by relocating management and operational activities to their cloud service providers. One of the reasons is that businesses are no longer faced with having to constantly update their servers. The infrastructure is maintained by the service provider and updates happen automatically and are available the next time you log into the cloud even without the need to pay for or download an upgrade.[12] Also, there are no format incompatibilities in Cloud Computing.[13]

Also, cloud providers are equipped with solutions that can be utilized in a disaster scenario.[14] Cloud providers will have the capacity to ensure sustainability through an unexpected event. So, unlike desktop computing, Cloud Computing eliminates the concern of losing valuable data when a hard disk crashes because all data is still accessible in the cloud.

Cloud Computing also enables users to access all their applications and documents from anywhere in the world. As applications and data are stored on distant servers rather than on users' own hard drives, users can access and store information wherever they are as long as they have Internet access, rather than having to remain at their desks.[15]

---

[6] Ben Rothke, "Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives," <http://www.slideshare.net/Benrothke/cloud-computing-business-benefits-with-security-governance-and-assurance-perspectives?src=related_normal&rel=561242> [Rothke].

[7] Miller, *supra* note 3, where Miller states that individuals' PC can be less expensive with a small hard disk, less memory, and more efficient processor as no software programs have to be loaded and no document files need to be saved.

[8] Salesforce, "What is Cloud Computing," <http://www.salesforce.com/cloudcomputing/>.

[9] *Ibid.*

[10] Rothke, supra note 6, where Rothke states that instead of waiting for weeks or months as the traditional IT models requires, users can just log in, customize it and start using it.

[11] *Ibid.*

[12] Leif, "Advantages of Cloud Computing," <http://contactdubai.com/webhosting/advantages-of-cloud-computing>.

[13] Miller, *supra* note 3, where Miller states that unlike where Word 2007 documents cannot be opened on a computer running Word 2003, all documents created by Cloud Computing can be read by any other user accessing the application.

[14] Rothke, supra note 6, where Rothke states that Cloud Computing is the ultimate data saving computing.

[15] Jason Dick, "Cloud Computing – 10 Benefits for Your Business," *Ezine Articles*, <http://ezinearticles.com/?Cloud-Computing---10-Benefits-For-Your-Business&id=3498637>.

As attractive as it sounds, there are plenty of motivations for startups and ordinary businesses to use the cloud and Cloud Computing has grown from being a promising business concept to one of the fastest growing segment of the IT industry. But, there are a number of legal considerations that bear careful consideration, but first and foremost of these are issues relating to privacy and personal information. As a chief security strategist of Hewlett-Packard cautioned, "there's a lot of power in the cloud, and with that power comes the ability to quickly get lost."[16]

Part II Cloud Computing and Privacy – PIPEDA's Implications

A. Outsourcing and Cross-Boundary Issues

(a) PIPEDA

Principle 4.1.3 of the *Personal Information Protection and Electronic Documents Act*[17] 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. Where organizations transfer data for processing, they must provide a comparable level of privacy protection for the data through contractual or other means. Accordingly, in order to comply with PIPEDA, organizations that transfer personal information must obtain sufficient contractual protections from third parties prior to transferral.

Principle 7(3)(c) enables an organization to disclose persona information where it is required "… to comply with a subpoena or warrant issued or an order made by a court person or body with jurisdiction to compel the production of information …".

Principle 7(3)(c.1) permits disclosure to a government institution without consent where the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law.

Combined, these obligations suggest that organizations seeking to of Cloud Computing services to the public on a commercial basis will need to comply with PIPEDA.

(b) Privacy Concerns in Cloud Computing

The use of third party contractors to manage information technology and data has increased dramatically in recent years because outsourcing is considered more efficient and effective. But the growing popularity of outsourcing coincides with the public's heightened sensitivity to privacy protection. When information can be stored anywhere in the cloud, the physical location of the information can become an issue because physical location dictates jurisdiction and legal obligations.[18] People and businesses may well find confidential, sensitive or personal information in the hands of unexpected third parties, including those of foreign governments.[19] The American *Patriot Act*[20] and

---

[16] Michael S. Mimoso, "Security News: Cloud Security Alliance Releases Top Cloud Computing Security Threats,": SearchSecurity.com, <http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1395924,00.html>.
[17] S.C. 2000. c. 5 [PIPEDA].
[18] Jennifer Stoddart, "Panel: Security, Privacy and Accountability: Remarks at the ICCP Technology Foresight Forum on Cloud Computing," (2009) Privacy Commissioner of Canada, < http://www.priv.gc.ca/speech/2009/sp-d_20091014_e.cfm> [Stoddart].
[19] Jeffrey F. Rayport, "Envisioning the Cloud: The Next Computing Paradigm," online: (2009) Marketspace Point of View at 40, <http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf>, where Rayport states that an individual's private information may actually be under the jurisdiction of another country, with laws very different from Canada.

other intelligence-related laws off U.S. authorities legal access to information over U.S. soil without requiring notification.[21] To avoid this, governments have made attempts to route Internet traffic away from U.S. jurisdiction and store their data outside the U.S. – Swift's attempts to locate its data center in Switzerland to keep European information on the Continent to prevent potential inquiries by the U.S. government offers one such example.[22] French authorities also banned use of blackberry devices by government officials to secure sensitive French national security information.[23] A Canadian example includes the *Freedom of Information and Protection of Privacy Amendment Act* passed by the B.C. government to temper public concern on data outsourcing.[24] Clearly, the issue of data outsourcing and privacy protection has become a global issue with concerns expressed in many different jurisdictions worldwide.

(c) Canadian Approaches to Outsourcing Canadians' Personal Information

Canadian privacy laws reach into foreign jurisdictions where there is a real and substantial connection to the parties or the substance of the transaction. In *Lawson* v. *Accusearch Inc*., the issue was whether the Privacy Commissioner was vested with the authority to investigate complaints against foreign organizations that collected, used, and sold the personal information of Canadians.[25] Ms. Lawson alleged that Abika.com routinely collected, used and disclosed personal information about Canadians for inappropriate purposes and without their knowledge or consent. Abika.com was a division of a corporation with its principal place of business in Wyoming. Ms. Lawson alleged that Abika.com, although based in the United States, violated PIPEDA. The court held that PIPEDA gives the Privacy Commissioner jurisdiction to investigate complaints relating to the trans-border flow of personal information as long as there is a real and substantial connection with Canada.[26] The decision is consistent with the Supreme Court of Canada's approach, reaffirmed in *Beals v. Saldanha*; however, based on the idea of international comity, this approach is subject to the legislature of the foreign jurisdiction adopting a different approach by statute.[27]

Consistent with the decision in *Abika*, a number of finding of the Privacy Commissioner illustrate the principle that an outsourcing company is obliged to provide a level of protection comparable to that required under PIPEDA by putting in place adequate contractual provisions with its foreign third party service provider. However, this protection will be subject to the laws of the foreign country.[28] In a

---

[20] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obsturct Terrorism Act of 2001*, Pub. L. 107-56, 115 Stat. 272.
[21] *Ibid*.
[22] *Ibid.* at 45.
[23] *Ibid.*
[24] Michael Geist, "Outsourcing our Privacy?: Privacy and Security in a Borderless Commercial World," (2005), 54 U.N.B.L.J. 272, at 277 [Geist].
[25] *Lawson* v. *Accusearch Inc*., 2005 4 F.C.R. 314 (2007). Ms. Lawson, a Canadian citizen, came across a website "abika.com" which offered a variety of search services on individuals including background checks, psychological profiles, phone numbers, automobile license plate details and criminal records. These searches were offered without the consent of the individual who was the subject of the search and not limited to Americans, but extended to persons in Canada.
[26] *Ibid.*
[27] *Beals* v. *Saldanha*, 2003, 3 S.C.R. 416.
[28] PIPEDA Case Summary 2008-394, "Outsourcing of Canada.com email services to U.S.-based firm raises questions for subscribers," The Office of Privacy Commissioner of Canada, <http://www.priv.gc.ca/cf-dc/2008/394_20080807_e.cfm>. Canada.com, owned and operated by Canwest, outsourced its email operations to a third party provider in the U.S. Through the contractual provision between Canwest and the third party provider in the U.S., Canwest maintained custody and control of the information that is processed by the U.S. provider by continuing oversight, monitoring, and audit of the services as if the service provider was located within Canadian borders. The Assistant Commissioner found that the respondent fulfilled its obligations to provide comparable protection under the Act by putting in place adequate contractual provisions, it is, however, impossible for Canwest to use contractual provisions to override the provisions of the U.S. statute.

subsequent case, the Assistant Commissioner found that PIPEDA cannot prevent U.S. authorities from lawfully accessing the personal information of Canadians held by organizations in the United States and that PIPEDA only demands that organizations protect customer personal information in the hands of foreign based third party service providers to the extent possible by contractual means.[29]

(d) PIPEDA Reforms

The touchstone for Canadian data protection is accountability, rather than geographical limits.[30] Wherever in the cloud the information may be, the use of Canadian's personal information must meet Canadian legal standards. There may be two options to reform PIPEDA to meet the challenge of the vulnerability of Canadians' personal information to foreign government aquisition: the creation of a blocking statute, and a stronger PIPEDA to increase its deterrent value against disclosure.[31]

A blocking statute is one that prevents compliance by a domestic entity with a specific foreign law. The inclusion of a blocking provision in PIPEDA could potentially protect the privacy rights of Canadians against disclosures to a government of a foreign jurisdiction and would present a strong Canadian defence against disclosures to foreign law enforcement.[32] Successful blocking statutes include Switzerland's financial privacy law,[33] which has proved resilient against attempts for disclosure of documents in the possession of Swiss banks. A Canadian example is the Foreign Extraterritorial Measures Act, which prevents Canadian corporations from complying with disclosure order issued as part of a foreign antitrust or international trade action without permission of Canada's Attorney General.[34]

Alternatively, a more proactive provision could be introduced to PIPEDA. Recently, a new restrictions on extra-jurisdictional data processing has been introduced in Canada. In British Columbia, Bill 73 was proposed to amend the *Freedom of Information and Protection of Privacy Act* (FOIPPA)[35] to require that all British Columbia public sector entities ensure that any personal information is stored and accessed only in Canada. It includes a prohibition on the transfer of personal information in the control of a public body outside Canada for data management, and requires that service providers notify the government when foreign government makes a disclosure request. The Alberta government also passed Bill 20 to amend the Alberta FOIPPA by making it an offence to comply with a subpoena, warrant or order "having no jurisdiction in Alberta to compel the production of information or pursuant to a rule of court not binding in Alberta."[36]

---

[29] PIPEDA Case Summary 2005-313, "Bank's notification to customers triggers *Patriot Act* concerns," The Office of Privacy commissioner of Canada, <http://www.priv.gc.ca/cf-dc/2005/313_20051019_e.cfm>.
[30] Stoddart, *supra* note 18.
[31] Geist, *supra* note 24.
[32] *Ibid*.
[33] *Ibid*.
[34] *Ibid*.
[35] John Beardwood, "New Canadian Restrictions on Extra-Jurisdictional Data Processing: Foreign Service Providers Take Note," Fasken Martineau DuMoulin LLP, <http://www.cba.org/CBA/newsletters/pdf/PRIV-Patriot.pdf>.
[36] Jason Young, "BC Attempts to Regulate International Outsourcing of Personal Information," Deeth Williams Wall <http://www.dww.com/?page_id=1052>.

B. Use and Disclosure

(a) PIPEDA

Use and disclosure of personal information by Cloud Computing service provides implicates a number of provisions of PIPEDA.

Principle 4.2.3 states that the identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected.

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.

Principle 4.3.2 clarifies that 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.

Principle 4.3.3 states that an organization shall not, as a condition of service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

Principle 5.3 states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

(b) Privacy Concerns in Cloud Computing

When a person stores information with a third party, the information may have fewer or weaker privacy protections than when the information remains only in the possession of the person. Secondary use or disclosure of information by a cloud provider has potential to expand the use of information in ways users can not anticipate.[37] The concerns include users' personal data being sold to another organization, being used in marketing campaigns and being analyzed and used to serve them with targeted advertising.

A common practice of cloud computing service providers is targeted online advertising. A user's information might contain useful data about others and a cloud provider can still market to non-users who show up in the user's records.[38] Similarly, a cloud provider may utilize its users' online profile or behaviour to third parties so that ads relevant to their apparent interests can be served to them.[39] Electronic health records (EHR) offer another example: service providers may accumulate medical data of patients to improve their availability and completion and to increase the efficiency of business processes for medical services; however, EHRs also support the secondary use of health data such as clinical studies, validation and post market surveillance of drugs.[40] Usually, health record privacy laws or other privacy laws may place limits on the usage and disclosure of personal information. The *Health*

---

[37] Robert Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," The World Privacy Forum, <http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf> at 21.
[38] *Ibid.*
[39] John Horrigan, "Cloud Computing Gains in Currency," PEW Internet & American Life Project <http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency>.
[40] Business & Information Systems Engineering, BISE, <http://www.bise-journal.org/index.php;do=show/site=wi/sid=12439520604bae19e60a08b674449530/alloc=16/id=95/area=>.

Insurance Portability and Accountability Act[41] and the German Act for the Modernization of the Health Insurance by Law[42] are such examples. But, they fail to provide mechanisms to guarantee the compliance of the EHR system regarding the enforcement of patient's decisions and patients cannot postulate or enforce obligations on further usage and disclosure of their data after an authorized disclosure. Canada also has health information privacy legislation in Ontario, the *Personal Health Information Protection Act*,[43] which applies to all health care information. PHIPA places obligations on health information custodians regarding the collection, use and disclosure on such information. However, with Cloud Computing, as data is accessible wherever the Internet is available, the data could be potentially seized through a party who has access to the Cloud Computing service. As a result, there are potential issues arising from the use and disclosure of health information under PHIPA.[44]

(c) Canadian Approaches to Use and Disclosure of Personal Information

Findings of the Privacy Commissioner conform that PIPEDA's rules in respect of the use and disclosure of Canadian's personal information will apply to Cloud Computing services, even where those services are located outside of Canada. In *CIPPIC v. Facebook*, the Privacy Commissioner was asked to consider Facebook's treatment of Canadians' personal information through its social networking service – a service that operates "in the cloud". The findings included that Facebook was not making a reasonable effort to notify users clearly that it used their personal information for advertising purposes in violation of Principle 4.3.2.[45] Facebook was also found to violate Principles 4.2.3 in that it was not providing users with sufficient time of collection notification of its use of advertising.[46] The Assistant Privacy Commissioner reasoned that privacy information related to purposes for collection and use of personal information should be gathered and explained fully in an organization's privacy policy and that Facebook has to be more transparent with users about its advertising practices.[47] In addition, the Assistant Privacy Commissioner found that Facebook, in violation of 4.2, made available all of a user's personal information accessible to a third party and that users lack control of their potential information insofar as no consent is sought from them for the disclosure of their personal information.[48]

Similarly, in *Lawson v. Accusearch*, the Commissioner found that in contravention of Principle 4.3, Abika – an American business with no offices or presence in Canada – collected, used, and disclosed the personal information of individuals living in Canada without their knowledge and consent.[49] The Commissioner also found that Abika has contravened 5.3 by collecting, using and disclosing personal

---

[41] *Health Insurance Portability and Accountability Act of 1996*, Pub. L. 104-191, 110 Stat. 1936.
[42] Federal Ministry of Health (2003), 'Gesetz zur Modernisierung der Gesetzlichen Krankenversicherung (GKV-GMG)', Bundesgesetzblatt 2003 Teil I, No. 55, Bonn.
[43] *Personal Health Information Protection Act*, S.O. 2004, c. 3.
[44] James Kosa, "Privacy and Jurisdictional Issues Raised by Cloud Computing," Deeth Williams Wall LLP, <http://www.it-can.ca/direct/membersonly/2009ST/cloud-kosa-cheung.pdf>.
[45] PIPEDA Case Summary 2009-008, "Report of Findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic against Facebook Inc." The Office of Privacy commissioner of Canada, <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm>.
[46] *Ibid*.
[47] *Ibid*.
[48] *Ibid.*
[49] Abika made more than 100 requests of vendors for the telephone records of persons living in Canada. It was further evidence that Abika did not make any effort to ensure the knowledge or consent of the individuals whose personal information is requested.

information of Canadians for purposes that a reasonable person would consider inappropriate in the circumstances.[50]

(d) PIPEDA Compliance

The essence of privacy protection is identifying the primary purposes for which the information is collected, and limiting the use to that purpose. PIPEDA compliance suggests that companies should embed in their systems restrictions on the kinds of uses that they may make of collected data. Similarly, companies engaging in cloud services should only collect the data that they absolutely need to provide the service.[51]

C. Data Retention

Cloud computing relies upon retention of a user's data by another party, whether that data be email, or work product, or even personal information belonging to someone else entirely. In addition to the question of what other uses a cloud provider will find for user data, it is crucial to consider whether the provider will take advantage of their capability to retain and make use of users' information, even after the users themselves are done with it. PIPEDA's principles call for the destruction or anonymization of data no longer required to fulfil the explicitly identified purposes of its collection,[52] and for guidelines to govern minimum and maximum periods of retention.[53] However, the surrender of control inherent to Cloud Computing raises possibilities that any privacy authority must be vigilant for – because they are possibilities that businesses, and less scrupulous authorities, can exploit.

Of course, data retention is a concern because it enables data use, and thus these concerns flow mainly out of the concerns about use. Wide-scale data retention by cloud providers underpins attempts at targeted advertising and data mining, for example. Such advertising, as has been pointed out by scholars such as Christopher Soghoian,[54] lies at the root of many consumer cloud providers' business models and enables their services to be provided at no cost to the end user. However, more esoteric uses have also been found for such data, and will continue to be found. Google, as an illustrative example of consumer cloud providers, has described how they use their wealth of user data to refine algorithms for translation and spell checking, as well as abuse analysis and other fields they see as "fundamental to bring value to our users."[55] The use such stored data may be put to can be bounded only by human ingenuity – which is why regulators must be on top of innovations in these fields.

Google itself notes that a policy of anonymizing data after a given period of time is one way to restrain these uses. Their current policy is to obfuscate IP addresses[56] after nine months and anonymize the unique cookie associated with a given data point after 18 months. Justifying this policy, Google privacy engineer Alma Whitten said that they had tried to work with a zero retention period and found

---

[50] Abika has provided no evidence that it has any policy, or makes any practices, of screening requests for information according to the appropriateness of the requestors' purposes. In some cases, its customers have requested non-public telephone records of other individuals to investigate the activites of current or former partners in a relationship.

[51] Ann Cavoukian, "Vidoe Transcript: On Cloud Privacy – Interview with Dr. Ann Cavoukian," An ROI Innovation Report, <http://www.itreportcanada.ca/itpublic/On_Cloud_Privacy.pdf>.

[52] PIPEDA, supra note 17, Schedule 1, Clause 4.5.3.

[53] *Ibid.*, clause 4.5.2.

[54] Christopher Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era", <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1421553> [Soghoian].

[55] Nate Anderson, "Why Google keeps your data forever, tracks you with ads", *Ars Technica*, March 7, 2010, <http://arstechnica.com/tech-policy/news/2010/03/google-keeps-your-data-to-learn-from-good-guys-fight-off-bad-guys.ars>

[56] Specifically, they remove the last octet of the IP address, changing from a unique identifier to a "one of 256 possibilities" identifier.

it untenable, and that even at nine months, "we believe that we have lost the ability to do things" that they find useful. Nine months is, in short, a compromise to Google – they would prefer even longer.

While Google's competitors, such as Microsoft and Yahoo, have sought to position themselves as more concerned about privacy for competitive advantage,[57] market forces cannot be entirely relied upon to drive adequate privacy protections in the consumer cloud market. The dominant business model for these services still relies on exploiting user data, and it is necessary to ensure that users are aware of the uses their cloud providers find for their information and able to provide meaningful consent for those uses – or enforce a withdrawal of that consent.

A second area of concern is government access to data retained by cloud providers. While only telecommunications providers are currently *required* to retain data on their customers for use by law enforcement (and even here only in the European Union per the *Data Retention Directive*[58]), many jurisdictions (particularly the United States) make it easier for law enforcement to access data held by a third party than it would be to access data that remained in the direct possession of the consumer – often requiring a simple subpoena instead of a search warrant.[59]

This proposition has not been directly tested in Canadian courts, but a close analog can be found in the Alberta case *R v. Weir*,[60] where an ISP's customer was held to have a reasonable expectation of privacy in their e-mail stored on the ISP's servers. The Weir ruling, along with PIPEDA principle 4.1.3, suggests that changes in the physical location and control of information do not change the legal protections that information is subject to, both from private actors and from governments. However, cloud providers, much like ISPs and telecom providers, will become tempting targets for security conscious governments due to the sheer concentration of potentially useful data.

D. Data Security and Technical Safeguards

When users relinquish control over their data to cloud providers, they also relinquish direct control over its protection. As such, the ability of cloud providers to prevent unauthorized access is a major element of user privacy.

PIPEDA's principles call for safeguards commensurate with the sensitivity of the information, including "technological safeguards, such as passwords and encryption."[61] However, Soghoian among others suggests that not everything that can be done to secure data storage and data transfers is being done, particularly in the consumer context.[62]

The transfer of data to or from a cloud user is, predctably, the weakest link. Soghoian focuses on typically unencrypted network connections to consumer cloud services.[63] However, authentication is as much an issue as transmission. Even if unencrypted data transfers are avoided, the traditional

---

[57] See for example this Microsoft release: <http://edge.technet.com/Media/Google-Chrome-steals-your-privacy/>.
[58] EC, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, [2006] O.J. L 105/54.
[59] Several American technology companies have recently formed the "Digital Due Process Coalition" to lobby for changes to the law to close this loophole: see <http://news.cnet.com/8301-13578_3-20001393-38.html>.
[60] 1998 ABQB 56, aff'd 2001 ABCA 181
[61] PIPEDA, Schedule 1, Clause 4.7.2-3.
[62] Soghoian *supra* note 54.
[63] While one of his major examples, Gmail, switched to default-encrypted network connections recently in response to an infamous set of intrusion attempts, this does not take away from the broader point.

username-password authentication method is vulnerable to phishing attacks and keyloggers, among other attack vectors.

Whether in securing the transmitted data itself, or simply authenticating the user, the same trade-off is being made: security versus usability and convenience. Soghoian notes that using encrypted networking protocols to cloud services would slow access down by 5-7 times on the user end, and significantly increase hardware costs on the provider end in order to provide the same level of service. Similarly, while security professionals note several less vulnerable authentication methods than the typical username/password scheme, they argue that "usability is a key issue to the adoption and maintenance"[64] of any new security or authentication scheme.

The enterprise market is an edifying example here. In this context, the ability to trust a provider with sensitive data is a salient selling point. Enterprise cloud providers cultivate and highlight their technical expertise, including in security,[65] and enterprise customers react to it. Market forces react predictably here, and an important reason for that predictability is that enterprise clients are almost viscerally aware of the danger facing them, what they can do about it, and what they can expect a provider to do about it – and they will go elsewhere if a provider does not meet those expectations, regardless of other perks.

This is the converse of Soghoian's argument that the consumer cloud business model does not provide incentives for consumer cloud providers to be serious about security. Consumer providers aren't, because consumers often aren't. Enterprise clients are, to the extent that it's often the first question they ask. If consumers can be brought to that same level of security consciousness – not just of the threats, but of the means to combat them and what their providers can and should do - then the incentives for cloud providers to be lax on security in favour of speed or storage space disappear.

On the other hand, consumers may not have the luxury to educate themselves in such a fashion. Soghoian discusses the reluctance of users to alter default security and privacy settings on Facebook, or the cookie settings in their web browsers. In the same way – and for the same reason – that social networking sites have been asked to mandate more secure defaults, so too should cloud providers. Existing private sector regulators may play a role addressing failures of marketplace incentives; technical safeguards in the consumer cloud market offer a textbook example of the need for regulators to play a such a role.

Part III Conclusion

A robust privacy protection framework should centre on accountability, not merely physical control and location. When one looks at privacy in this way, the physical abstraction that is inherent in Cloud Computing stops mattering.

Someone – the cloud provider – still controls the data, no matter where it is located. For privacy law and regulation to deal with Cloud Computing, it needs to provide regulatory authorities with the tools to hold providers accountable, through flexible concepts of jurisdiction. It must provide consumers with the tools to hold providers accountable. Accountability will arise through service provider disclosure and transparency on its use of data, and through regulators – and consumers through lawsuits

[64] Richard Duncan, "An Overview of Different Authentication Methods and Protocols", *SANS Institute Reading Room*, <http://www.sans.org/reading_room/whitepapers/authentication/overview-authentication-methods-protocols_118>.
[65] See for example the comments from Google and Amazon executives to CNET at <http://news.cnet.com/8301-1009_3-10150569-83.html>.

and complaints to regulators – raising awareness about security risks and mitigation techniques. And the law must restrain providers from taking advantage of their users, through strong mandates against abuse of the physical control service providers enjoy over this data.

Cloud computing does not present a challenge of law: offsite data storage is nothing new, and the PIPEDA regime is well on the way to considering location irrelevant relative to control and responsibility. What Cloud Computing *does* present is a challenge of implementation and enforcement, but it is a challenge that can and must be met.

Appendix: Selected Bibliography of Publications Addressing Cloud Computing and Privacy

Ann Cavoukian, "Video Transcript: On Cloud Privacy – Interview with Dr. Ann Cavoukian," online: An ROI Innovation Report <http://www.itreportcanada.ca/itpublic/On_Cloud_Privacy.pdf>.

Ann Cavoukian, "Privacy in the Clouds," online: Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf>.

Ben Rothke, "Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives," Online: Slideshare <http://www.slideshare.net/Benrothke/cloud-computing-business-benefits-with-security-governance-and-assurance-perspectives?src=related_normal&rel=561242>.

Business & Information Systems Engineering, online: BISE <http://www.bise-journal.org/index.php;do=show/site=wi/sid=12439520604bae19e60a08b674449530/alloc=16/id=95/area=>.

Charles Babcock, "Cloud Computing Differences Between U.S. and Europe," Online: InformationWeek <http://www.informationweek.com/cloud-computing/blog/archives/2010/04/cloud_computing_17.html?queryText=cloud+computing>.

Christopher Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era", online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1421553>.

Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," online: Educause Resources <http://www.educause.edu/Resources/SecurityGuidanceforCriticalAre/196517>.

David A. Couillard, "Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectation in Cloud Computing" (2009) 93 Minn. L. Rev. 1943.

Eric Knorr, "What Cloud Computing Really Means," online: Cloud Computing <http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031>.

James Keller, "Web-based computing spurs privacy concerns," online: The Globe and Mail <http://www.theglobeandmail.com/news/technology/article975051.ece>.

James Kosa, "Privacy and Jurisdictional Issues Raised by Cloud Computing," online: Deeth Williams Wall LLP <http://www.it-can.ca/direct/membersonly/2009ST/cloud-kosa-cheung.pdf>.

Jason Dick, "Cloud Computing – 10 Benefits for Your Business," online: Ezine Articles <http://ezinearticles.com/?Cloud-Computing---10-Benefits-For-Your-Business&id=3498637>.

Jason Young, "BC Attempts to Regulate International Outsourcing of Personal Information," online: Deeth Williams Wall < http://www.dww.com/?page_id=1052>.

Jeffrey F. Rayport, "Envisioning the Cloud: The Next Computing Paradigm," online: (2009) Marketspace Point of View at 40, <http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf>.

Jennifer Stoddart, "Panel: Security, Privacy and Accountability: Remarks at the ICCP Technology Foresight Forum on Cloud Computing," online: (2009) Privacy Commissioner of Canada < http://www.priv.gc.ca/speech/2009/sp-d_20091014_e.cfm>.

John Beardwood, “New Canadian Restrictions on Extra-Jurisdictional Data Processing: Foreign Service Providers Take Note,” online: Fasken Martineau DuMoulin LLP < http://www.cba.org/CBA/newsletters/pdf/PRIV-Patriot.pdf>.

John Horrigan, “Cloud Computing Gains in Currency,” online: PEW Internet & American Life Project <http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency>.

Leif, “Advantages of Cloud Computing,” online: UK Dedicated Servers, Cloud Computing <http://contactdubai.com/webhosting/advantages-of-cloud-computing>.

McMillan Binch Mendelsohn, Privacy Law Bulletin: Parliamentary Committee Recommends Changes to PIPEDA, online: <http://www.mcmillan.ca/Upload/Publication/ParliamentaryCommitteeRecommendsChangestoPIPEDA_0707.pdf>.

Michael Geist, “Outsourcing our Privacy?: Privacy and Security in a Borderless Commercial World,” (2005), 54 U.N.B.L.J. 272.

Michael Miller, “Cloud Computing Pros and Cons for End Users,” online: Inform IT <http://www.informit.com/articles/article.aspx?p=1324280>.

Michael S. Mimoso, “Security News: Cloud Security Alliance Releases Top Cloud Computing Security Threats,” online: SearchSecurity.com <http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1395924,00.html>.

Nate Anderson, “Why Google keeps your data forever, tracks you with ads”, *Ars Technica*, March 7, 2010, online: <http://arstechnica.com/tech-policy/news/2010/03/google-keeps-your-data-to-learn-from-good-guys-fight-off-bad-guys.ars>.

Office of the Privacy Commissioner of Canada, “Reaching for the Clouds: Privacy Issues Related to Cloud Computing,” online: Reports and Publications <http://priv.gc.ca/information/pub/cc_201003_e.cfm>.

Robert Gellman, “Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing,” online: The World Privacy Forum <http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf>.

Richard Duncan, “An Overview of Different Authentication Methods and Protocols”, *SANS Institute Reading Room*, online: <http://www.sans.org/reading_room/whitepapers/authentication/overview-authentication-methods-protocols_118>.

Simon Hodgett, “Cloud Computing Raises Privacy Concerns,” *The Lawyers Weekly*, 28:37, (13, February 2009).