Regulating the Cloud: A Comparative Analysis of the Current and Proposed Privacy Frameworks in Canada and the European Union

David Krebs[*]

ABSTRACT

Cloud computing is a growing phenomenon and promises greater efficiency and reduced-cost computing. However, some of the basic technological and business-related features of the Cloud are at odds with personal data protection laws. Canada and the European Union share similar core values related to privacy/data protection, and both regions aim to increase their competitiveness regarding cloud computing. Having these two similarities in mind, this paper explores the current legal and stakeholder landscape in Canada and the European Union with respect to cloud computing, data protection and how adoption of the model can be advanced.

The analysis shows that neither of the frameworks is entirely compatible with cloud computing in its current application. Canada's legal landscape is slightly more hospitable, but is lacking direction from regulators, while the EU's non-harmonized and restrictive framework presents a challenge for cloud proliferation. Relevant stakeholders have diverging views on how data protection in the Cloud should be approached and 2012 will be a year during which these views will likely be debated in detail, in particular in response to the draft proposal of the European Commission on a new data protection framework. This paper concludes with distilling four possible options in this regard.

I. INTRODUCTION

> *The cloud sort of is part of that Internet gift. It's the next step, it's the next phase, it's the next transition, and depending on who you are, and how you think, you could say the cloud started five years ago, ten years ago. You can go back to 1969, if you want, and say that the cloud started 40 years ago, because the microprocessor and the Internet are the gifts that just keep on giving us the chance, and the opportunities to make a difference.*[1]

Microsoft CEO Steve Ballmer's comments provide an indication of why *everyone* is talking about "the Cloud". Cloud computing has been hailed as promising

---

[*] J.D. University of Saskatchewan. LL.M. candidate, Stockholm University. Member of the Bar of Alberta. Currently working in Uppsala, Sweden.

[1] Microsoft, "Remarks made by Steve Ballmer, CEO, at a speech at the University of Washington", March 4, 2010, online: Microsoft <http://www.microsoft.com/presspass/exec/steve/2010/03-04cloud.mspx>.

to be a major part of the future of information communications technology[2] and as a fundamental trend of the Internet — itself recently described as the "most disruptive technology we will have seen in history".[3] Others have referred to it as nothing but a fancy term for time-sharing models that have been around since the 1960's.[4] The other side of the debate lies in the weighing of the benefits and dangers involved in deploying the model, in particular when it comes to sensitive data. Champions of the Cloud, like Microsoft's CEO, see it as having unparalleled potential of revolutionizing the way in which we communicate and store and access data, software programs and technology infrastructure,[5] whereas skeptics view it as a large-scale threat to personal privacy and information security.[6]

Whatever view one shares, the protection of electronically stored personal data is one of the most salient topics in the discussions surrounding cloud computing and how, when, and if it should be widely adopted. In Western jurisdictions, privacy and data protection legislation was conceived, drafted and implemented before the term "cloud computing" came into existence. It was, therefore, not designed to necessarily accommodate situations where personal data is moved freely from one jurisdiction to another (often unbeknownst to the individual), accessed over the Internet or where it shares server space with other parties, all of which may be the case where an organization stores data with a cloud service provider ("CSP").

This paper explores how stakeholders in Canada and in the European Union ("EU") are evaluating data protection[7] and the particular legal challenges of storing personal data in the Cloud. This comparison is of interest because of Canada's rela-

---

2 Expert Group Report for the European Commission: Information Society and Media, Jeffrey, K. and Neidecker-Lutz, B (eds.), "The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010", online: European Commission <http://cordis.europa.eu/fp7/ict/ssai/Docs/cloud-report-final.pdf>.

3 Comments made by Eric Schmidt, CEO at Google, during the Activate 2010 Conference referring to how the Internet has turned an economy of scarcity to one of abundance, online: The Guardian <http://www.guardian.co.uk/media/video/2010/jul/02/google-eric-schmidt-activate>.

4 See Bruce Schneier, "Be Careful When You Put Your Trust in Cloud Computing", The Guardian, (June 4, 2009), online: The Guardian <http://www.guardian.co.uk/technology/2009/jun/04/bruce-schneier-cloud-computing>.

5 See Schmidt Comments, *supra* and Future of Cloud Computing, *supra*.

6 See Christopher Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era" (2009) Vol. 8 J. On Telecomm & High Tech. L. 359 at 361.

7 This paper will be using terminology from both the Canadian and European legal realm. That is, the terms "privacy protection" and "personal information" will be used alongside the European terminology "data protection" and "personal data" and where in Canada one speaks of an *individual's* personal information, under European law this person is referred to as a "data subject". The same goes for the Canadian terminology of "using, collecting and disclosing" of information being referred to generally as "processing".

tionship with the "EU" and the mutually shared values on privacy.[8] Canada's private sector privacy legislation, the *Personal Information Protection and Electronics Documents Act*[9] ("PIPEDA"), was implemented to conform to European privacy legislation[10] (and has been deemed as offering "adequate" protection under the European Data Protection Directive),[11] and the developments in Europe are therefore an important gauge for Canadian policy and business interests. Conversely, Canada has been viewed as providing a third alternative to data protection[12] compared with the US industry self-regulating approach and the more strict regulatory environment of the EU, and may therefore be of interest to European legislators, as well as to industry wishing to use service providers in Canada. Both regions are also vying for a spot among the leaders in the ICT arena and are competing as desirable locations for the growing cloud computing market. The legal framework in each country and region may partially determine where cloud providers will move and where the technology will be embraced.[13]

Within the EU, particular attention will be paid to the current debate in Germany and, to a lesser extent, Sweden; Germany, because it is Europe's largest economy and a leader in the ICT field in Europe, and it has one of the most successful privacy regimes[14] and Sweden because it was the first country to enact data protection legislation in Europe[15] and it is another European leader in the ICT industry.

Currently, the data protection regulatory framework in EU Member States, let alone across the globe, is not harmonized and, in fact, quite fragmented. CSPs have been making it known that this needs to change if cloud computing is to reach across-the-board acceptance, and trust. Organizations and providers will need to know their respective obligations in order to be compliant in their operations and this in turn will ultimately affect willingness to adopt the technology.[16] Conversely,

---

8 The similarities have been well-documented. See e.g. Michael Zimmer, "Privacy Protection in the Next Digital Decade: "Trading Up" or a "Race to the Bottom"?" in *The Next Digital Decade* at 477.

9 S.C., 2000, c.5.

10 See, e.g. Jeremy Warner, "The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps", [2005] 2 UOLTJ 75.

11 Council Directive 95/46, 1995 O.J. (L 281) 31–39 (EC) (Oct. 24, 1995), online: EurLex <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.

12 Lee Bygrave, "Privacy Protection in a Global Context", *Scandinavian Studies in IT Law*, ed. Peter Wahlgren (Stockholm Institute for Scandinavian Law: 2004, Vol. 47) at 340.

13 See Michael Geist, "Location Matters Up in the Cloud", Toronto Star (December 10, 2010) online: Toronto Star <http://www.thestar.com/business/article/901068 — geist-location-matters-up-in-the-cloud#article>.

14 Bygrave, *supra* at 345.

15 *Datalagen*, 1973.

16 Jeremy Kirk, "Ballmer Calls for Clearer Data Rules from Europe", PC World (November 4, 2010), online: PC World <http://www.pcworld.com/businesscenter/article/209722/ballmer_calls_for_clearer_data_rulesfrom_europe.html>.

Privacy Commissioners are among those who have voiced concerns about the model and whether or not cloud computing can ever be compliant with the current data protection frameworks as they exist, *inter alia*, in Canada and Europe.

In order to analyze these matters appropriately, this paper is divided into four parts. The first part will provide a brief overview of the cloud model as understood in 2011. The second part will canvass the threats cloud computing poses to electronically stored personal information by describing the model's features underlying these threats.[17] The discussion will then move on to describe and contrast the current landscape, consisting of laws, and stakeholder proposals and opinions relevant to the central issues surrounding the protection of personal information in cloud computing. The ultimate goal will then be to compare, contrast, and analyze the current and potential future landscape and how it might affect the adoption of a feasible framework for the protection of personal data stored in the Cloud.

Much has been written over the past three years about data protection in the Cloud and the intended contribution of this paper is not to make an exhaustive inventory of the Cloud's threats to personal privacy. It is to summarize, analyze and contrast the current legal landscapes in Canada and in Europe in order to distill commonalities and differences which may then enable an enlightened look, into 2012 and beyond, of how the regulation of data protection in the Cloud might develop.

II. THE NATURE OF CLOUD COMPUTING

To state that there are more than a few definitions of cloud computing would be a great understatement. Cloud computing is an "evolving paradigm"[18] and its definition will change, very likely from time when this article was commenced until it was finalized.[19] For current purposes suffice it to say that, essentially, cloud services include the provision of scalable (adjusted according to need) services that allow individuals and businesses to access and use, via the Internet, software and hardware, which is managed or owned by third party service providers.[20] Instead of keeping information stored locally on the home desktop or on a server in the office, customers using cloud services store their information remotely, usually on shared servers owned by others, and there are often more than one CSP involved in this

---

17 The Canadian definition of personal information means information related to an identifiable individual, the European Data Protection Directive speaks of "[. . .]". In this paper I will be using the term "personal information" as referring to all jurisdictions, pointing out potential differences where applicable.

18 Peter Mell and Tim Grance, "The NIST definition of Cloud Computing, Version 15", National Institute of Standards and Technology, online: NIST lt;http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>.

19 In fact, the NIST has recently released an updated version of the definition discussed herein.

20 Also see Office of the Privacy Commissioner of Canada, "Draft Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing", Office of the Privacy Commissioner of Canada, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/resource/consultations/report_2010_e.cfm#ftnref32>.

process (i.e. second or third-tier subcontractor CSPs). In terms of its application, the sky (no pun intended) is the limit. Small and medium sized firms, large corporations, governments, as well as law firms are all types of organizations that are or may in the not-too-distant future be using cloud services.

(a) Benefits of Cloud Computing

Cloud computing can be categorized as SaaS, PaaS and IaaS, referring, respectively, to Software, Platform and Infrastructure "as a service". Broadly speaking, IaaS is a service that provides access to hardware via the Internet, SaaS is usually provided by allowing access to software applications via the Internet (rather than installing these on internal hardware), while PaaS allows the customer to write and execute software code on the Cloud infrastructure. These services can be combined or provided separately.[21] A customer using SaaS leaves much of the control of his technology (and data) to the CSP while retaining relatively more of this control using IaaS and PaaS.[22] This is called choosing levels of "abstraction".

The Cloud can be deployed in different ways either as a private (internal or external), community,[23] public or a hybrid cloud.[24] The way in which the Cloud itself is deployed is of crucial importance to the nature and extent of the related privacy concerns. With the public cloud model, the infrastructure is available to the general public. One or more clouds may be stored on the same physical server and accessed through virtualization. This is a central feature but also one that creates the highest level of concern. With the private internal model, cloud technologies are deployed across an organization and the customer retains all control over security, hardware and software, whereas with an external model this control is passed to the CSP. A hybrid model is a model that exists but for which no standardized definition has been determined as of date.[25] Essentially, it combines other cloud mod-

---

21 For a more detailed description, see NIST, *supra*.

22 Joep Ruiter and Martijn Warnier, "Privacy Regulations for Cloud Computing Compliance and Implementation in Theory and Practice" (2010) at 3, online: IIDS <http://www.iids.org/aigaion/? page=publication&kind=single&ID=316>.

23 "The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise." See NIST, *supra*.

24 Also see Wikipedia "Cloud Computing" online: Wikipedia <http://en.wikipedia.org/wiki/Cloud_computing#Private_cloud>.

25 *Ibid*: "*There is some confusion over the term "Hybrid" when applied to the cloud — **a standard definition of the term "Hybrid Cloud" has not yet emerged**. The term "Hybrid Cloud" has been used to mean either two separate clouds joined together (public, private, internal or external), or a combination of virtualized cloud server instances used together with real physical hardware. The most correct definition of the term "Hybrid Cloud" is probably the use of physical hardware and virtualized cloud server instances together to provide a single common service*." Compare with definition in Ruiter, *supra*: "*Hybrid Clouds are a combination of the other Cloud types. In a hybrid Cloud, organizations use a CSP in cases where additional resources are required*." and that of the NIST: "*The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by*

els so one ends up either with two of them joined together or with virtual infrastructures that are combined with physical hardware.

The benefits of using cloud technologies, or at least the extent thereof, are not entirely uncontested,[26] but mainly relate to cost, efficiency and flexibility of use. Customers using cloud technologies do not need to make capital investments such as for networks and hardware but rather pay on a needs basis. This also provides a related benefit of the flexibility to use services *ad hoc*, when they are needed (scalability/on-demand services).[27] These benefits are derived from, *inter alia*, the pooling of resources and virtualization. That is, different organizations, using separate cloud infrastructures, share the same hardware but only use the resources they require at a given time. Although somewhat contradictory to the discussion herein regarding the biggest threats to data, the Cloud may actually promise *increased* security for some businesses, especially small and medium sized businesses that may not have otherwise had the resources to invest in security measures.[28] Similarly, some believe that privacy may actually be improved by cloud computing through increased use of and innovation regarding privacy-by-design efforts as well as the data protection capabilities of CSPs as compared with customers.[29]

The reasons underlying the Cloud's advantages are closely related to its drawbacks and the concerns related to its use, particularly with respect to data protection. The model in and of itself has characteristics that cannot be amended in order to protect data because it is those characteristics which make the Cloud viable in the first place.

(b) The Threats to Personal Information

It is trite to say that personal information is at risk of becoming compromised no matter where it is stored. Whatever risks exist, they are increased when information is transacted and stored in the Cloud. The threats most commonly associated with cloud computing are unlawful access by computer hackers, lawful interception/access by governments (not to mention covert government action), service continuity, rights to and responsibility for data, international transfer of data/jurisdiction and of course various issues surrounding security of clouds in gen-

---

standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds), *supra*."

26 See e.g. Mimecast, "Cloud Barometer Survey", Mimecast, online: Mimecast <http://www.mimecast.com/barometerresearch2010, and Office of the Information and Privacy Commissioner, "Reaching for the Clouds", online: Office of the Privacy Commissioner of Canada www.priv.gc.ca/information/pub/cc_201003_e.cfm>.

27 See NIST's description of On-demand self-service, Resource pooling. Rapid elasticity, Measured Service, *supra*.

28 Andrew DeVore, "Cloud Computing: Privacy Storm on the Horizon?" (20. Alb. L.J. Sci. & Tech. 365, 2010) at 366.

29 Office of the Privacy Commissioner of Canada, "Draft Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing" (October 25, 2010), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/resource/consultations/report_2010_e.cfm>.

eral, which is considered the biggest overall threat in the Cloud.[30] More particularly, attacks on personal data, and therefore also on the privacy of the individual, have been categorized as one of the biggest threats to cloud computing by members of the cloud computing industry.[31] Data is more susceptible to becoming "compromised" due to the number of interactions online as well as the architecture and technology of the Cloud itself. This section does not intend to provide an exhaustive list of all threats posed by the Cloud but rather it will distill an overview of the most common issues that arise from the use of cloud computing, being threats stemming from the architecture of the model and those arising out of business decisions made by CSPs and their customers and suppliers.

(i) Inherent Features

As we have noted previously, the cloud model is based on the sharing of scalable resources. "Multi-tenancy" is one essential inherent feature of this model and means that a number of virtual machines are hosted on one physical server. Many individual computers (from potentially many parts of the world) communicate with the main terminal which is located at a separate location. Two distinct concerns have been noted here. One cloud may become the target by another sitting on the same server, something known as a "side-channel attack".[32] The second related issue is unauthorized access to data by law enforcement officials. If one virtual machine is the subject of an authorized (or unauthorized) seizure all other clouds sitting on the physical machine will also be seized and could potentially be accessed.[33] The issues accompanying this threat are twofold: one being that there is a potential breach or privacy (and related matters such as potential disclosure of intellectual property and other sensitive data) and the second being interrupted access, which is both of legal and business concern.

Another feature is the so-called "Cloud stack",[34] whereby layers are stacked on top of one another. Each layer may involve the provisioning of services by a separate CSP. The obvious threat here is that more and more parties are involved in the process of collecting, using, storing and disclosing (personal) data. With each new party involved and with each layer of abstraction, the data subject (individual) loses part control over his personal data. Also, each layer of the stack could be hosted in a different location and/or jurisdiction, and thus, more and more of the

---

30 There is an abundance of commentary available about these issues online. For a good overview of the main issues see Cloud Security Alliance "Top Threats to Cloud computing, Version 1.0", March 2010, online: Cloud Security Alliance www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

31 *Ibid* at 12.

32 See Ken Choo, "Cloud Computing: Challenges and Future Directions", Australian Government: Trends & Issues in Crime and Criminal Justice, No. 400 (October, 2010). In such an attack, the cache of the target machine may be monitored, and thus data taken, quite easily after mapping the internal cloud structure to identify where the target cloud resides on the server.

33 *Ibid*.

34 See e.g. "Cloud Stack", Wkipedia, online at <http://en.wikipedia.org/wiki/File:Cloud_Computing-_Stack.svg, last accessed on January 10, 2011>.

control over data is given up by the client to the cloud provider(s), who themselves may not always be able to easily locate the data within the cloud structure.[35] However, threats to privacy and security do not only emerge in the Cloud because of the nature of the model, they also arise because of the business decisions the CSP and customer make relating to their contracting relationship and the technology used.

(ii) Business Decisions

CSPs and their customers are free to contract on some of the terms they wish that are unaffected by the technology of the Cloud. These business decisions will either increase or decrease the threats to personal data. As an example, encryption technologies are by some experts[36] seen as a viable way to protect data in the Cloud. CSPs could decide to use encryption or they could decide to send information over the Internet in its original form, for anyone intercepting the communication to be able to read. In practice, encryption technologies are not always utilized appropriately, or at all, due to various reasons relating to cost or lack of system sophistication, or simply because industry has no real incentive to provide for network encryption.[37] When logging on to Facebook's site, the user after logging in is still connecting with an (unsecure) "http" rather than a encrypted "https" connection.[38] The reason for this is not entirely clear. This may be due to the lack of incentive (or lack of perceived consumer demand) or that pages take longer to load when encrypted, but it may also be that some Internet based business models depend on the lack of encryption for advertising and data mining purposes.[39] Other examples of where cloud-specific measures may be the cause of privacy issues are insufficient authentication, authorization, and audit controls; operational failures; data center reliability and inappropriate disaster recovery.[40] If the Cloud is not protected in line with the latest security technology it leaves data vulnerable to both lawful and unlawful access.

From a business perspective, the chosen contractual arrangements may also pose a threat to data stored in the Cloud. For example, an agreement may provide for customer data to be disclosed under certain circumstances but not put the obligation on the CSP to notify the customer if such disclosure was to occur (provided that the law allows for such an arrangement).[41] Another scenario can arise where

---

35 IBM, "IBM Point of View: Security and Cloud Computing (Whitepaper)" (November 2009), online IBM <http://www.ibm.com/common/ssi/fcgi-bin/ssialiasinfotype=SA&subtype=WH&appname=SWGE_TI_SE_USEN&htmlfid=TIW14045USEN&attachment=TIW14045USEN_HR.PDF>.

36 Refer to discussion infra.

37 Caught in the Cloud, *supra* note 3 at 392.

38 This is due to change, although consumers will have to change the setting themselves, see Matthew Schwartz, "Facebook boosts security", Information Week, online: Information Week, <http://www.informationweek.com/news/security/app-security/showArticle.jhtml?articleID=229100364>.

39 *Ibid* at 395 ff.

40 Top Ten Threats, *supra* note 21.

41 See e.g. Amazon, "Amazon Web Services Customer Agreement", section 10.2, online: Amazon aws.amazon.com/agreement/:

contractual arrangements are subject to change (much like many Terms of Use or privacy policies online) without notice to the customer. At signing, the customer may have been onside his legal duties with respect to personal data under his control but if terms, such as where data is stored, change without notice compliance with privacy laws vanish.[42]

As we have seen, there are many different models for which the Cloud can be used. With the public cloud model, data is often stored in a third country[43] and, if such is the case, there occurs a transfer of data from one jurisdiction to another. Data belonging to one organization (and the personal information of individuals within that organization), which is entrusted to the Cloud, could be stored on the same server as that of another organization, which may or may not be based in another jurisdiction. That is, the physical location of the server, holding data of individuals from countries A and B, might be in country C.

The private cloud set-up may also be such that data is stored off-site and in another country, but this is not necessarily the case. Generally speaking, a private cloud will be less susceptible to the threats to personal data stored thereon than will a public cloud, and a hybrid cloud infrastructure will lie somewhere in the middle of the security scale. The threats to personal information can then be said to in-or decreased on account of (business) decisions, such as preferring one cloud model to the other, deciding on the type — and location — of cloud provider or the level of abstraction in terms of the layers within the Cloud (i.e. choosing IaaS, PaaS, SaaS or all three in some form).

(c) Technology and Policy-based Solutions

As will be discussed later, there are currently many proposals surrounding the black letter of data protection laws that would suit the cloud model. But this is not the only, or possibly the best, way of protecting personal data. This paper will not explore technological solutions in detail (especially from a technical perspective) but it is important to describe the main methods currently being discussed in Canada, the EU, and elsewhere in this context to understand some of the proposals made from a legal standpoint.

One technology-based solution is data encryption, where personal data is en-

---

> We will not disclose Your Content, except: (i) if you expressly authorize us to do in connection with your use of the Services; or (ii) as necessary to provide the Services to you, or to comply with the Agreement or the request of a governmental or regulatory body, subpoenas or court orders.

42 As an example, where data is hosted in cloud the physical location of which moves from one jurisdiction to another and the second jurisdiction is not compliant with those laws the customer is subject to (transfer of data outside of the EU To jurisdiction not deemed "adequate").

43 See e.g. iWire, "Microsoft Calls for APEC Harmony", October 21, 2010, iWire, online: iWire <http://www.itwire.com/it-policy-news/government-tech-policy/42599 -microsoft-calls-for-apec-cloud-harmony?start=1>, where it is stated that Microsoft Australia is said to be storing Australians' data in the Cloud with data of that Cloud stored in Singapore.

crypted before it is sent into the Cloud. This may be an effective way of protecting data in IaaS and PaaS applications but in SaaS models, it may render the data unusable for the CSP.[44] As will be described in more detail in 3.1.3., the "privacy-by-design" model attempts to address this issue by introducing external verification and authentication methods so that encrypted data can be accessed and used by CSPs.

From a general policy perspective, some, including industry, advocate a use-based model, whereby personal information's legitimate use is central, and not "privacy" worries.[45] Instead of aiming at limiting use and curbing the market for information, it should rather be embraced. Closely tied to this method is the transparency and industry-standards approach, which is being advocated by industry players. Another approach that has come to the forefront recently is the "audit approach",[46] which aims to enforce accountability through rigid electronic monitoring and enforcement of breaches. Personal data ownership, that is, attaching property rights to personal information, has also been widely debated,[47] advocated and also dismissed by some. So far, personal information has not been deemed "property" either in Canada or in the EU.

III. LEGAL FRAMEWORK, PROPOSALS AND VIEWS

The Office of the Privacy Commissioner of Canada ("OPC") has distilled a list of nine so-called "privacy risks of Cloud Computing":[48] jurisdiction, creation of new data streams, security, data intrusion, lawful access, processing, misuse of processing data, permanence of data and ownership of data. Regulating trans-border flows of data from country to country has also been cited as a central issue.[49] Peter Schaar, Information and Privacy Commissioner for Germany, considers the main issue to be that neither the data subject nor the data controller may know where data is located at any given time[50] and that, on a base level, privacy laws are not able to cope with this model at all. Industry actors have maintained that the core issues surrounding cloud computing and data protection are related to security and lack of transparency of security practices,[51] and cohesive, consistent, and harmo-

---

44 Privacy Regulations for Cloud Computing, *supra* at 9.

45 Larry Downes, "A Market Approach to Privacy Policy", in Berin Szoka and Adam Marcus, eds., *The Next Digital Decade: Essays on the Future of the Internet*, (TechFreedom: 2010) at 524–26.

46 Michael Zimmer, *supra*, at 502.

47 For a pro and con debate, compare Michael Zimmer, *supra* and Lawrence Lessig, *Code 2.0*, (Basic Books: New York, 2006) on this topic.

48 Reaching for the Clouds at 5-6.

49 For a comprehensive discussion of transborder data flows, see Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law" (TILT Law & Technology Working Paper, No. 016/2010), October 2010, Version 1.0.

50 Peter Schaar, "Data Protection Must not Disappear in the Cloud" (July 19, 2010), Bund fur Datenschutz, online: Bund fur Datenschutz <http://www.bfdi.bund.de/cln_136/EN/PublicRelations/SpeechesAndInterviews/blog/DatenschutzDarfNichtInDerCloudVerschwinden.html>.

51 IBM Whitepaper, *supra*, at 5.

nized regulatory frameworks.[52]

For the purposes of the first part of the following discussion, I will focus on how legislation, current and proposed, is suitable for protecting personal data by discussing five core issues: cross-border transfer of data, data intrusion, lawful access and jurisdiction, as well as the status of CSPs with respect to the responsibility for the personal data they process. The discussion will then move on to exploring the views of industry and privacy commissioners to lead into the final part of this paper, which is the comparative analysis of the different approaches and where these may lead to in 2012 and beyond.

When contemplating ways to regulate novel issues or changing technology, legislators are faced with challenging task: they must regulate without the benefit of having had years of experience to look back on and they may be pressured to act quickly. This is case with cloud computing. It has been stated that five rationalities compete in this respect: the political, legal, cultural, and operative rationalities, and finally, the internal rationality.[53] The nature of these rationalities may be similar across countries or they may be very different. The manner in which regulators will ultimately decide to address data in regard to cloud computing might depend most prominently on the industry itself, public opinion, privacy overseeing bodies and other privacy experts, the views of law enforcement and, finally, on the political goals of government. While this paper will not be conducting a step-by-step analysis of all of the factors in the competing rationalities — it could instead be said to canvass the legal and political rationalities in Canada and the EU while pointing out gaps that may affect the operational and internal rationalities-, nor will all relevant players here be surveyed, but it is nonetheless worthwhile to keep this approach in mind while moving forward in our analysis of the potential for workable, cloud-ready data protection schemes in Canada and the EU.

(a) Canada

This paper will not delve into the details of privacy in international law but it is important to note the basic framework and to briefly set out current international initiatives as they form the basis of and are mutually influential with the Canadian and EU frameworks. To begin with, there is currently no official international data protection authority. There is also no overarching authority or association to which

---

52 Brad Smith (General Counsel, Microsoft Corporation), "Building Confidence in the Cloud: A Proposal for Industry and Government Action for Europe to Reap the Benefits of Cloud Computing", January 2010, online: European Commission ec.europa.eu/justice/news/. . ./microsoft_corporation_2nd_document_en.pdf, last accessed on January 15, 2011.

53 See Peter Wahlgren, "The Legitimacy Sphere: Between Law, Culture, Politics and Enforceability", in Scandinavian Studies in Law, Vol 56 (Stockholm Institute for Scandinavian Law & Peter Wahlgren: 2010) at 427. The political rationality means that laws must operate practically in a democratic society, and the operational rationality that laws must be enforceable (and possible to follow and uphold) while the legal aspect suggests that these laws must then also be acceptable from a legal perspective. The cultural rationality relates to how laws are received within a country's or region's culture. Finally, the internal rationality focuses on the laws' internal logic, i.e. are they contradictory or do they contains important gaps?

complaints can be brought, as, for example, in the intellectual property realm.[54] However, the data protection schemes in Canada and the EU, as well as other countries, are based on common principles, as first pronounced by the OECD in 1980.[55] There are also initiatives, such as the Madrid Resolution[56] and the Global Privacy Enforcement Network,[57] which all mark a growing effort on behalf of data protection authorities to reach out to one another and to further international cooperation and the development of standards. Legislation may be a long way from becoming harmonized across the (Western) world but this is not stopping international initiatives by data protection authorities to address the issues. The views of these regulatory authorities have been fairly consistent regarding the articulation of the core privacy and data protection principles are as well as what problems, in their view, need to be addressed in the Web 2.0 world.[58]

Canada is a privacy conscious country and as Dr. Cavoukin, current Information and Privacy Officer of Ontario ("IPC"), wrote in 2006, "Self-defense of personal privacy is a growing movement, no longer limited to the actions of a few privacy hawks."[59] Canada also has a vibrant ICT sector and Canada's government and industry have ambitious plans in terms of Canada's role in the global market. Canada, much like other parts of the world, is concerned about, and interested in curbing, crime, including crime using or based on the Internet. These realities can

---

54 Where a patent applicant may register a patent with World Intellectual Property Organization ("WIPO") and claim priority for his invention.

55 OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", OECD, online: OECD <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>.

56 International Conference of Data Protection and Privacy Commissioners, "International Standards on the Protection of Personal Data and Privacy", November 5th, 2009, online: Privacy Conference <http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf>.

57 Members are U.S. Federal Trade Commission, Office of the Privacy Commissioner of Canada, Commission Nationale de l'Informatique et des Libertés (France), Office of the Privacy Commissioner, New Zealand, Israeli Law, Information and Technology Authority, Office of the Privacy Commissioner, Australia, Office of the Data Protection Commissioner, Ireland, Agencia Española de Protección de Datos (Spain), Information Commissioner's Office (United Kingdom), Garante Per La Protezione Dei Dati Personali (Italy), Dutch Data Protection Authority (the Netherlands), Federal Commissioner for Data Protection and Freedom of Information (Germany), Office of the Victorian Privacy Commissioner, (Victoria, Australia).

58 See e.g. Office of the Canadian Privacy Commissioner, "Joint Letter to Google" (April 19, 2010) OPC, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm>.

59 Dr. Ann Cavoukian and Don Tapscott, "Privacy and the Enterprise 2.0" (IT & CA: October 17, 2006), New Paradigm Learning Corporation, online: New Paradigm Learning Corporation newparadigm.com/media/Privacy_and_the_Enterprise_2.0.pdf, last accessed on January 10, 2011.

at times be at odds[60] with one another when it comes to data protection, working at opposite ends of the spectrum. But can there be symbiotic effects? That is, can the aims of industry, privacy hawks, privacy overseeing bodies and government be reconciled with the effect of creating a cloud model that provides a mutually recognized adequate data protection framework?

(i) Current Legislation

Canada's Constitution gives jurisdiction over privacy matters to the federal and the provincial governments. The public and private sectors are governed by separate pieces of legislation at a federal and provincial level. Nationally, PIPEDA governs private sector organizations while the *Privacy Act*[61] governs the public sphere at a federal level. The Provinces each have separate public sector legislation but only four (Alberta, Saskatchewan, Manitoba and Ontario) have specific[62] health-sector legislation. Essentially, PIPEDA applies to the processing of personal information relating to all commercial activities where there is no provincial private-sector legislation, as well as to inter-provincial and international personal data flows, but it does not regulate activities related to the personal information of employees of provincially regulated organizations. Non-profit organizations in relation to their non-commercial activities are also not regulated by PIPEDA.[63]

At a provincial private-sector level, only Alberta, Quebec and British Columbia have enacted their own pieces of commercial private-sector legislation, and within those Provinces, PIPEDA only applies to federally regulated organizations, including the personal information of employees of those federal organizations. Alberta and British Columbia legislation specifically regulates the use of personal information of employees.[64] The Quebec act does not differentiate between employee and non-employee personal data.[65]

This means that a federally regulated company operating in Alberta would be regulated by both PIPEDA — regarding non-employee personal information- and the provincial legislation regarding activities related to personal employee information. As a result, Canada does not have an entirely uniform data protection framework. Compared with the EU (where Member States themselves, such as for example Germany, may have a federal-provincial system comparable to that of

---

60 For a discussion surrounding Google's Street View and Buzz products and their reception by the international privacy community see e.g. Joint Letter to Google, *supra*, and *Preliminary Letter of Findings, October 19, 2010 — Complaints under PIPEDA against Google Inc.*, Office of the Privacy Commissioner of Canada, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm, last accessed on January 10, 2011>.

61 R.S., 1985, c. P-21.

62 In British Columbia, for example, the private-sector act is intended to cover the health sector.

63 Whereas, for example, the Alberta PIPA does apply to non-profits but exempts non-commercial use of personal information.

64 *Personal Information Protection Act*, SBC, c. 63, 2003, s. 13.

65 *An Act respecting the Protection of personal information in the private sector*, RSQ, c P-39.1.

Canadian), however, these differences are still quite minor and one can speak of a relatively cohesive approach throughout the country. It is important to stress that this statement must be viewed in the context of a comparison with the landscape in the EU. There are indeed differences within Canada as to how personal information may be used, collected and disclosed, but the manner in which the private sector is regulated by PIPEDA and provincial legislation is cohesive in that common principles and a common culture underlie the regulations. PIPEDA applies (subject to the exceptions noted above) across the entire country while within the EU, the Data Protection Directive did not have so-called "direct effect". Rather it forms the model on which Member States were to base their respective laws, which has led to 27 different variations of that same piece of legislation. This is also one of the main drivers behind the proposal for a new harmonized European privacy framework envisioning a "Regulation"[66] with direct effect on EU Member States (more on this proposal under section 3.2.1.).

As we have seen, the Cloud introduces a third actor (at minimum) into the data protection realm. Rather than just having a collector and a provider of personal information, in the Cloud there is a third-party actor who is, as Ontario's Privacy Commissioner states, "outside of . . . [the] trusted security perimeter".[67] This model is not to be confused with a regular outsourcing arrangement. These two may share some common traits — like the need to establish contracts that outline security measures regarding the processing of personal information- but the CSP-customer relationship is based on the *ad hoc* exchange of data and services via the Internet, while the outsourcing relationship is based on a point-to-point delivery of services. Privacy legislation must accommodate this new reality and this section will canvass PIPEDA's provisions for its "Cloud readiness", that is, how Canada's current legal framework addresses, or is suited to tackle, core cloud-related privacy issues such as transfer of data into third countries, data intrusion, lawful access and jurisdiction.

(A) Trans-border Transfer

With some minor exceptions,[68] Canadian privacy laws generally do not restrict the transfer of personal data to third countries. In contrast to the EU, at a federal level Canada has chosen the "organization-to-organization",[69] rather than the state-to-state approach to regulate the transfer of personal information within the private sector. While PIPEDA does not restrict the transfer of personal information to other jurisdictions, it does place the obligation on the transferring organiza-

---

66 EC, *Proposal for a Regulation of the European Parliament and Council on the Protection of inviduals with regard to the processing of personal data and the free movement on such data (General Data Protection Regulation)*, 2012/0011(COD).

67 Privacy by Design, *supra* at 5.

68 There are some provincial restrictions in certain instances with respect to information in the hands of public bodies, as well as special rules regarding the storage of financial information, e.g. s. 239 *Bank Act, S.C. 1991, c. 46*.

69 See Office of the Privacy Commissioner of Canada, *Guidelines for Processing Data Across Borders*, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm>.

tion to ensure a "comparable level" of protection while the information is being processed by a third party (including those active in another country).[70] The OPC has confirmed this in numerous recent decisions[71] and has also released guidelines[72] for businesses in this respect, including further clarification on what constitutes a "comparable level of protection".[73] The OPC has confirmed that a "transfer" is not a "disclosure" but rather a "use" under PIPEDA, which would *not* require renewed consent from the data subject.[74] The OPC believes that *PIPEDA* does not require amendment in terms of the cross-border transfer of data in cloud computing:

> We have long stated that we believe that privacy does not hinder innovation and economic progress. The organization-to-organization approach that underscores PIPEDA supports transborder flows and data protection by holding organizations to account for their personal information protection practices. Information is accessible to authorities regardless of where it resides. As noted in our Guidelines, we do, however, maintain our view that a careful risk assessment needs to be undertaken prior to any arrangement that involves the outsourcing of personal data to other organizations that operate globally, and that this assessment should consider the legal requirements of the jurisdiction in which the third-party processor operates, as well as some of the political, economic and social conditions, and any additional risk factors, in that jurisdiction.[75]

While an organization is not obliged to obtain renewed consent from individuals it is under an obligation to provide notice that information might be transferred outside of the country. In practice, organizations are making explicit mention of the

---

70 Principle 4.1.3. of Schedule 1.

71 See *PIPEDA Case Summaries 2008 — #313 and #365*.

72 Office of the Information and Privacy Commissioner, "Guidelines for Processing Data Across Borders", Office of the Privacy Commissioner of Canada, online at <http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm>, last accessed on January 12, 2011.

73 *Ibid*: "Comparable level of protection" means that the third party processor must provide protection that can be compared to the level of protection the personal information would receive if it had not been transferred. It does not mean that the protections must be the same across the board but it does mean that they should be generally equivalent."

74 *PIPEDA Case Summary 2008-#394*: "With regard to the issue of customer consent, the Office has taken the position that the sharing of information with a third-party service provider constitutes a "use" for the purposes of the *Act*. Organizations obtain customer consent for the use of personal information for the provision of services or products when individuals first apply for the service or product. Although service providers may change over time, if the purpose of the current provider's use of the personal information has remained the same, organizations are not required to obtain renewed customer consent for the information use. (emphasis added)."

75 Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing, (May, 2011), online: IPC <http://www.priv.gc.ca/resource/consultations/report_201105_e.cfm#toc6c>.

USA Patriot Act[76] as the threat of having US authorities access this data (by virtue of an Order under that Act) is many times the main cause of concern for Canadians to have their data stored in the United States.[77] Indeed, it has been stated that the *USA Patriot Act* is a main obstacle toward main-stream adoption of cloud computing not just in Canada, but on a European and also global scale.[78] This is despite the fact that many agree that legislation in other countries very similar to[79] and thus just as threatening to privacy as the *Patriot Act*. On this very issue, the OPC has noted that:

> The risk of a U.S.-based service provider being ordered to disclose personal information to U.S. authorities is not a risk unique to U.S. organizations. In the national security and anti-terrorism context, *Canadian organizations are subject to (and may be just as likely to receive) similar types of orders to disclose personal information of Canadians to Canadian authorities*. There are also several formal bilateral agreements in place between analogous Canadian and U.S. organizations that provide for the cooperation and exchange of relevant information. In light of such arrangements, there are many alternatives to a Section 215 Order to obtain information about Canadians (emphasis added).[80]

Canada's approach puts the onus to safeguard personal information on the transferring organization, without imposing any absolute restrictions based on the transferee's country of establishment. This approach obviously suits cloud computing because it does not prohibit a transfer into another country *per se* but focuses on the organization's practices itself. But that is not the end of the matter. The Cloud brings with it an *ad hoc* outsourcing model. That is, data is transferred into and downloaded from the Cloud by users *ad hoc*; data moves freely between customer and CSP, including potential second and third-tier sub-contractor CSPs, data centres. Also, the location of the data may not always be known to the customer, and other parties, who are potentially also unknown to the customer, may be processing customer data. If such is the case, the "openness" and "transparency" principles, which form the basis of Canadian (and most international) privacy law, cannot readily be guaranteed, at least not under the current understanding of those principles, notwithstanding the organization-to-organization approach. One must also remember that cloud computing challenges global privacy principles, such as the OECD Guidelines, which were not intended to accommodate the Internet as we know it today,[81] but a point-to-point transfer of data.

One important distinction that needs to be made when discussing the rules surrounding transfer of personal data to third-countries is that under PIPEDA, as noted, consent is required from the data subject, irrespective of whether the data subject is an employee or another individual whose information is under the control

---

76 115 Stat. 272 (2001).

77 See *PIPEDA Case Summary 2008-#394*, *supra*.

78 Paul Lanois, "Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?" (Nw. J. Tech. & Intell. Prop. L., Vol. 9 No. 2, November 2010) at 45.

79 *Ibid* at 46.

80 *PIPEDA Case Summary 2008-#*394, *supra*.

81 Transborder Flows, *supra*, at 10.

of the regulated organization. Under Alberta and BC private sector legislation, the transfer of "personal employee information" does not require the consent of the employee, but instead relies on a reasonable and notice standard.[82] For a provincially regulated organization with operations in multiple Provinces this means that the requirements might differ from Province to Province as it might be subject to PIPA regarding personal employee information in Alberta but PIPEDA regarding customer personal information that is transferred across Canadian borders, not to mention the gap in legislation regarding personal employee information in Provinces without private sector privacy legislation (e.g. Saskatchewan).[83]

(B) Data Intrusion

Data intrusion occurs when there is an unauthorized access to data, usually stemming from a breach in the security system of an organization. A breach with respect to personal information occurs where there is an unauthorized disclosure, loss or access to, or a theft of, personally identifiable information. Strong breach notification laws are generally considered to play an important role in empowering individuals' right to privacy and to informational self-determination[84] in increasing the transparency of an organization's information handling practices. They also strengthen best practices of industry and the general public's awareness of the gravity (and sometimes scale) of breaches that would otherwise not have come to the forefront.[85]

Canadian privacy law, with the exception of Alberta's *Personal Information and Privacy Act*,[86] does not contain any mandatory breach notification provisions,

---

82 S. 18 PIPA: "An organization may use personal employee information about an individual without the consent of the individual if (a) the information is used solely for the purposes of (i) establishing, managing or terminating an employment or volunteer-work relationship, or (ii) managing a post-employment or post-volunteer-work relationship, between the organization and the individual, (b) it is reasonable to use the information for the particular purpose for which it is being used, and (c) in the case of an individual who is a current employee of the organization, the organization has, before using the information, provided the individual with reasonable notification that personal employee information about the individual is going to be used and of the purposes for which the information is going to be used."

83 For further information on this topic, see R. Gary Dickson, Q.C. and Sandra Barreth, "Privacy Laws and Virtue Testing in the Workplace" (2006), online: Office of the Information and Privacy Officer of Saskatchewan <http://www.oipc.sk.ca/Presentations/WorkplacePrivacyReport.pdf>.

84 See e.g. OPC Consultation Report at III.II.

85 Kenneth A. Bamberger & Deirdre K. Mulligan, "Privacy on the Ground" (2010) 63 Stan. L. Rev. (Draft) at 47, online: SSRN <http://ssrn.com/abstract=1568385>.

86 S.A. 2003, c. P-6.5, s. 34.1 "An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a *real risk of significant harm* to an individual as a result of the loss or unauthorized access or disclosure (emphasis added)."

yet at least. Bill C-29[87] proposes to change this and includes provisions requiring organizations to report breaches of a "material"[88] nature to the Commissioner and, in cases where the breach poses a "real risk of significant harm to the individual"[89] to the affected individuals. The proposed legislation imposes no penalties or other consequences for non-compliance with this section (in Alberta, the Commissioner can force an organization to comply)[90] and has therefore been criticized in academic as well as in practitioners' circles.[91] Apart from Bill C-29, the Government has also tabled Bill C-28, the *Fighting Internet and Wireless Spam Act*.[92] Which has just received royal assent (only parts are in force as of date). Its provisions are not controversial and are generally accepted as necessary and welcomed[93] changes to PIPEDA.

(C) Lawful Access

According to some, lawful access by governments is one of the most imminent and grave threats to personal data in the Cloud.[94] Digital technologies have enabled governments to monitor individuals on a large scale like never before in the history of surveillance technologies.[95] The architecture of the Cloud allows this surveillance to be accomplished with less cost and effort, and more surreptitiously.[96]

Under current legislation, the ability to gain lawful access to telecommunications is governed mainly by the *Criminal Code of Canada*,[97] the *Competition Act*[98] and *Canadian Security Intelligence Service Act*.[99] Canada currently does not have

---

87 *An Act to Amend the Personal Information Protection and Electronics Documents Act*, 3rd Session, 40th Parl., 2010.

88 *Ibid*, s. 11, adding s. 10.1 to PIPEDA.

89 *Ibid*, s. 10.2.

90 *Ibid*, s. 37.1.

91 Bill McKiernan, "New Federal privacy, anti-spam bill gets mixed reviews" (May 31, 2010) Law Times, online: Law Times <http://www.lawtimesnews.com/201005316982/Headline-News/New-federal-privacy-anti-spam-bills-get-mixed-reviews>.

92 3rd Session, 40th Parl., 2010.

93 See Jennifer Kavur, "Kudos for anti-spam bill, concern over PIPEDA changes", IT World, online: IT World <http://www.itworldcanada.com/news/kudos-for-anti-spam-bill-concern-over-pipeda-changes/140774> and Patricia Kosseim, "Federal Privacy Regulation in 2010: A Balance Sheet", Remarks at the 6th Annual Administrative Law and CLE Conference organized by the Osgoode Hall Law School, October 19, 2010, Office of the Privacy Commissioner of Canada, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/speech/2010/sp-d_20101019_pk_e.cfm>.

94 See Caught in the Cloud, *supra*.

95 *Ibid* at 384.

96 For more on this issue see Caught in the Cloud, *supra* Part III and Code 2.0, *supra* Chapter 5.

97 R.S. 1985, c. C-46.

98 R.S. 1985, c. C-34.

99 R.S., 1985, c. C-23.

legislation that requires ISPs to deliver subscriber information without a warrant or court order, maintain minimum data retention periods or that requires ISPs to retain subscriber information (such as traffic data). As it stands, data retention in Canada is governed only to the extent of its limitations. Principle 4.5 of PIPEDA states that "Personal information shall be retained only as long as necessary for the fulfillment of those purposes."

All lawful interception is subject to applicable privacy laws, such as PIPEDA and the *Privacy Act*, as well as section 8 of the *Canadian Charter of Rights and Freedoms*,[100] which guarantees the right to be free from unreasonable search and seizure. Under section 7(3) of PIPEDA, information may only be disclosed without consent in specific circumstances such as information sought to protect national security, under a warrant and other specified authority, or as required by law.

The *Criminal Code* sets out particular circumstances wherein telecommunications may be lawfully intercepted. Save for exceptional circumstances,[101] an application, *ex parte*, must be made by the government agent seeking to intercept a communication, either in Court or by way of telephone application (where an in-person application would not be feasible).[102] For some time now, the Canadian Government has been of the view that its laws in this respect are outdated[103] and need to be modernized in order to a) be in line with international commitments, such as the *Convention on Cybercrime*,[104] and b) to keep up with advancements in technology.[105] After initial consultations in 2005 and 2007, legislation aimed at addressing these, arguable, shortcomings were tabled in 2009.

This legislation was first introduced as Bill C-47, the *Technical Assistance for*

---

100 Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.

101 s. 184.4 "A peace officer may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication where (a) the peace officer believes on reasonable grounds that the urgency of the situation is such that an authorization could not, with reasonable diligence, be obtained under any other provision of this Part;(b) the peace officer believes on reasonable grounds that such an interception is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and(c) either the originator of the private communication or the person intended by the originator to receive it is the person who would perform the act that is likely to cause the harm or is the victim, or intended victim, of the harm."

102 *Ibid* at s.183.2.

103 See e.g. Parliament of Canada, "Lawful Access: the Legislative Situation in Canada", Parliament of Canada, online: Parliament of Canada <http://www2.parl.gc.ca/Content/LOP/ResearchPublications/prb0565-e.html>.

104 Council of Europe, *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through com–puter systems* (28 January 2003) online: UNHCR <http://www.unhcr.org/refworld/docid/47fdfb20f.html>.

105 See Department of Justice, "Lawful Access — Summary of Submissions to the Lawful Access Consultation", Department of Justice, online: Department of Justice <http://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html, last accessed on January 10, 2011>.

Law Enforcement in the 21st Century Act,[106] was aimed at assisting, along with Bill C-46,[107] law enforcement in gaining access to digital communications. The key measures of Bill C-47 have been summarized by the "Parliamentary Information and Research Service" as addressing:

> a concern expressed by law enforcement agencies, which contend that new technologies, particularly Internet communications, often present obstacles to lawful communications interception. The bill permits the following: It compels telecommunications service providers to have the capability to intercept communications made using their networks, regardless of the transmission technology used (clauses 6 to 15). It provides law enforcement agencies with access, under an accelerated administrative process without a warrant or court order, to basic information about telecommunications service subscribers. At the same time, the bill provides for certain protection measures (clauses 16 to 23).[108]

After progress of the Bills stalled somewhat after the First Reading in the House of Commons at the end of 2009, the Government in November of 2010 reintroduced the proposed legislation as Bill C-52,[109] along with Bills C-50[110] and C-51.[111] These three pieces of legislation have been said to introduce provisions that would "reshape Internet in Canada" based on mandated surveillance technologies, information disclosure, and new police powers.[112] The mandatory disclosure of information, as well as the type of "basic information" referred to above, is set forth in s. 16(1) of Bill C-47 (C-52):

> Every telecommunications service provider shall provide a person designated under subsection (3), on his or her written request, with any information in the service provider's possession or control respecting the name, address, telephone number and electronic mail address of any subscriber to any of the service provider's telecommunications services and the Internet protocol address, mobile Identification number, electronic serial number, local service provider identifier, international mobile equipment identity number, international mobile subscriber identity number and subscriber identity module card number that are associated with the subscriber's service and equipment.

The Privacy Commissioner retains explicit authority to audit the practices of the government officials under this legislation. What is interesting, however, is that

---

106 Canada, 2nd Session, 40th Parl., 2009.

107 *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Session, 40th Parl., 2009.

108 "Legislative Summary", LEGISinfo, online at <http://www2.parl.gc.ca/Sites/LOP/LEGISINFO/index.aspList=ls&Query=5887&Session=22&Language=e>.

109 *An Act regulating telecommunications facilities to support investigations*, 3rd Session, 40th Parl., 2010.

110 *An Act to Amend the Criminal Code (interception of private communications and related warrants and orders)*, 3rd Session, 40th Parl., 2010.

111 *Investigate Powers for the 21st Century Act*, 3rd Session, 40th Parl., 2010.

112 Michael Geist, "Lawful Access Bills Would Reshape Internet in Canada", Michael Geist blog, online: Michael Geist <http://www.michaelgeist.ca/content/view/5450/159/>.

an interception pursuant to s. 16(1) is stated to explicitly[113] fall under s. 7(3) of PIPEDA, which allows a disclosure which is "required by law", rather than s. 7(3)(c.1), which would obligate the requestor of personal information to establish its lawful authority to access the information under certain prescribed circumstances, such as for reasons of national security. Furthermore, the proposed legislation enables access without court supervision.

This Bill places more of an administrative and commercial burden[114] on ISPs while impeding on individuals' privacy rights. It also obliges ISPs to use the "means under its control" to decrypt messages but only if they were encrypted by that service provider. The Bill does not impose a general obligation to provide decrypted communications[115] but it does mandate an ISP to design its systems so that they may later be intercepted by law enforcement.[116] The threat to personal information under Bill C-47 is the ISP information mentioned above may be stored with other, more sensitive, data in a cloud infrastructure. By way of a lawful interception, law enforcement may gain access to data stored in the Cloud much more easily than would be the case in a traditional client-server infrastructure. Moreover, a CSP, and thus the cloud customer and data subjects, may not even be aware of this access.

This piece of legislation may very well be of concern for customers contemplating the use of a CSP in Canada. On the other hand, this legislation does create a framework under the auspices of the Privacy Commissioner, and the mere existence of a framework (as opposed to uncertainty) may provide increased comfort to the cloud community.

With the federal election in the Spring of 2011 the proposals (not having received royal assent) died on the Order Paper. However, similar legislation was recently re-introduced by the conservative government as Bill C-30 (short title: *Protecting Children from Internet Predators Act)*,[117] which received royal assent on March 23, 2012. The provisions to a large extent mirror previous proposals and remain the source of severe criticism by privacy advocates. Bill C-30 is said to give government a "stunning array of powers"[118] to spy on its citizens and the short title

---

113 Bill C-47, s. 23.

114 ISPs must implement systems in compliance with s. 7 of Bill C-52, including real-time surveillance capabilities.

115 s. 6(4): "Despite subsection (3), a telecommunications service provider is not required to make the form of an intercepted communication the same as it was before the communication was treated if (a) the service provider would be required to develop or acquire decryption techniques or decryption tools; or (b) the treatment is intended only for the purposes of generating a digital signature or for certifying a communication by a prescribed certification authority, and has not been used for any other purpose.

116 *Ibid*, s. 7.

117 *An Act to Enact the Investigating and Preventing Criminal Electronic Communications Act and to Amend the Criminal Code and Other Act*, 1st Session, 41st Parl., 2012.

118 Michael Geist, "*Why Bill C-30 Gives the Govt the Power To Install Its Own Surveillance Equipment on ISP Networks*", Feb 22, 2012, Michael Geist, online: www.michaelgeist.ca, referring to Section 14 of Bill C-30.

alone is stirring controversy. It is said to project an atmosphere of fear,[119] while being "disingenuous",[120] and used as a selling tool rather than a reflection of its aims.[121] The Liberal Party has stated that it is principally against warrantless searches and "will insist on committee hearings that ensure that all concerned groups are given the opportunity to comment on the proposed legislation. [. . .] judicial oversight (issuing of warrants) should be required in virtually all circumstances before a permit is issued for the gathering or sharing of an individual or organization's information."[122] Privacy advocacy groups have noted that "8 in 10" Canadians oppose the introduction of these laws.[123]

(D) Jurisdiction

In the Cloud data is uploaded, downloaded, stored and otherwise processed using the Internet as the main transportation and access medium. Data is often sent across jurisdictional boundaries and used in multiple locations, calling into question matters such as applicable law (where contract silent) and proper jurisdiction for launching of complaints.

Recent decisions in Canada have brought some clarity to these issues. In *Lawson v. Accusearch Inc.*[124] the matter before the Federal Court was whether or not the Commissioner had jurisdiction to investigate a complaint against a US company that was allegedly processing information of Canadians in contravention of PIPEDA. The Court held that the Commissioner indeed had jurisdiction over the complaint on account of the "substantial connection" to Canada (individuals were resident in Canada) and the nature of the subject matter. This means that an organization located outside of Canada, but collecting (or otherwise processing) data from Canadians (in the course of commercial activities) may be subject to the jurisdiction of the OPC.[125]

The OPC is of the view that complaints brought by individuals against a CSP will fall under her jurisdiction when "the assessment indicates that real and substantial connection to Canada exists".[126] To what extent this holds true will likely

---

119 Matt Hartley, "Comment: Canada's embarrassing failure on lawful access legislation", Feb 14, 2012, National Post, online: <http://business.financialpost.com/2012/02/14/comment-canadas-embarrassing-failure-on-lawful-access-legislation/>.

120 Dr. Ann Cavoukian, as quoted in "Toews surprised by content of online surveillance bill" CBC, online: <http://www.cbc.ca/news/politics/story/2012/02/18/pol-thehouse-vic-toews.html>.

121 See e.g. "*Protecting Children from Internet Predators Act*", Wikipedia, online: <http://en.wikipedia.org/wiki/Protecting_Children_from_Internet_Predators_Act>.

122 Marc Garneau, Letter to Canadians, (October 31, 2011), Open Media, online at: <https://openmedia.ca/sites/openmedia.ca/files/SOS_LPCStatement_111104.pdf>.

123 Open Media, online: <http://openmedia.ca/news/liberals-join-8-out-10-canadians-standing-against-government%E2%80%99s-warrantless-online-spying-bills>.

124 2007 FC 125.

125 Note that in Canada, where contracts are entered into over the Internet, jurisdiction exists where Canada is either the Country of transmission or reception *SOCAN v. Canadian Ass'n of Internet Providers*, [2004] 2 S.C.R. 427 at 457.

126 Reaching for the Cloud(s), *supra*.

be explored in future decisions of the OPC and the Courts, but given the case law it is hard to imagine that a Canadian resident who has her data processed by a non-resident CSP will *not* be able to bring a complaint based on the CSPs alleged breach of PIPEDA. This rather clear legal framework should add to the comfort level of Canadians with respect to the use of cloud computing.

(E) Status of CSPs

Because cloud computing introduces a new actor into the data provider-data collector dynamic, even as compared with a traditional outsourcing relationship, the question of responsibility and accountability naturally arises. In Canada, there is less uncertainty about this issue than in the EU. The OPC has stated that it might investigate a complaint involving cloud computing in four situations, the nature of which will determine which actor will be responsible for complying with PIPEDA. The first complaint might arise where personal data is provided by a cloud customer to a CSP. Here, the OPC is clear that it considers this a "transfer for the purpose of processing" under Principle 4.1.3[127] and that the *customer of the CSP* will be held accountable for the handling of the personal data. However, the OPC also takes the position that where the CSP acts "outside the processing relationship", for example misuse or unauthorized access to data, that it will itself be responsible *vis-a-vis* the regulating authorities.[128] Appropriate cases have not come up as of yet but this assessment is a likely outcome. The third situation involving CSPs and personal information would be where a private person uses a cloud service such as a webmail or photo storage application, and those providers are in breach of their PIPEDA obligations. The final situation where a CSP may be responsible in the first instance arises for a private cloud structure in one organization. Again, the CSP would find itself in the position of the (initial) "data controller", to use the EU terminology. As will see in 3.2.1.5., the categorization in EU legislation is much less straightforward on this point.

(ii) Government Cloud Strategies

The Canadian Government was scheduled to launch its digital strategy, *Canada's Digital Economy Strategy*, in the spring of 2011. The five cornerstones of this strategy are set to include infrastructure, business adoption of digital technologies, Canadian business supplying digital products to the world, a skilled workforce and Canadian content on digital platforms.[129] To date, this strategy has still not

---

127 Schedule 1 of PIPEDA, being "*"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.*"

128 Reaching for the Cloud(s), *supra*.

129 "Minister Clement Updates Canadians on Canada's Digital Economy Strategy", Industry Canada News Release, online at www.ic.gc.ca/eic/ic1.nsf/eng/06096.html, last accessed on January 10, 2011.

been released by the government, which has been criticized heavily.[130] Without a concrete legal and technological strategy, Canada risks losing valuable ground both from an economic and consumer protection standpoint.

That, albeit important, point aside, part of the strategy is supposed to include new or updated legislation covering copyright (Bill C-32) (2nd Reading, but stalled since end of 2010), anti-spam (Bill C-28) (received royal assent, but only the sections amending complaints in PIPEDA have come into force) and privacy (Bill C-29) (First Reading, stalled since end of 2010), but the government has made hardly any progress on this front since the last election. With respect to privacy the strategy explains Bill C-29 as "protecting" and "empowering" consumers while "clarifying" and "streamlining" rules for businesses and "enabling" effective law enforcement. Cloud technologies are mentioned as specifically valuable for the government and the SME (small and medium-sized business) sectors.

The Canadian government has itself been slower[131] in moving services or internal processes into the Cloud than, for example, parts of the US administration.[132] Canada's CTO of Public Works presented a strategy[133] for the government's approach to cloud computing leadership in the Autumn of 2009. In his view, Canada has the potential for becoming a leader in the field:

> Due to its geographical characteristics, cooler temperatures and low-density population(particularly as one moves farther north in Canada), IT expertise, quality construction standards, legislative framework (including the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*) and low-cost green energy, Canada is considered a prime location for Cloud Computing. Canada has a reputation of being a highly desirable outsourcing location for companies from around the world because of factors such as our well-educated talent pool, multicultural population, geopolitical stability and relatively low cost of conducting business.

Since then, however, the process of ensuring Canada's leadership or at least competitiveness has stalled somewhat from the Government's side, whereas in other parts of the world, including the EU and the United States, the move towards government clouds and overall cloud strategies has intensified. This has led some commentators to worry that the lack of the government's lead, along with fears of storing data with American CSPs, will lead to Canada being left behind in the race

---

130 Michael Geist Keynote speech, Canada's Digital Strategy, "Hidden in Plain Sight", Michael Geist, online: <http://www.michaelgeist.ca/>.

131 See e.g. Rafael Ruffalo, "Canadian government catches up in Cloud at GTEC" (October 6, 2010) IT World Canada, online: IT World Canada <http://www.itworldcanada.com/news/canadian-government-catches-up-on-cloud-at-gtec/141672>.

132 See e.g. Darryl Taft, "Amazon Helps U.S. Government Move to the Cloud", May 14, 2010, eWeek, online: eWeek <http://www.eweek.com/c/a/Cloud-Computing/Amazon-Helps-US-Government-Move-to-the-Cloud-883856/>.

133 Jiri Danek (CTO of Canadian Public Works), "Cloud Computing and the Canadian Environment", Sribd, online: Scibd <http://www.scribd.com/doc/20818613/Cloud-Computing-and-the-Canadian-Environment#open_download>.

for becoming a leader in this field.[134] 2011 was supposed to provide more clarity in terms of the Canadian Government's proposals but as of present, the sense is that Canada, as compared to the EU and its Member States, lags behind in its articulation and implementation of a cloud vision, a view that is shared within industry.

(iii) Views of Privacy Commissioners

> Legal uncertainties make it difficult to assess the status of information in the cloud as well as the privacy and confidentiality protections available to users. *The law badly trails technology* and the application of old law to new technology can be unpredictable. For example, current laws that protect electronic communications may or may not apply to cloud computing communications or they may apply differently to different aspects of cloud computing.[135]

The above was written for an American audience but remains equally applicable here. The fact that laws need to be amended in order to accommodate Web 2.0 applications and business models seems to be universally accepted. Privacy laws may have been drafted vaguely so as to accommodate unforeseen future technologies but ultimately, they do not always match the requirements of cloud computing. The extent to which this adjustment needs to occur is not always uncontested. The OPC concluded a consultation process with the public and industry experts on current issues within privacy and data protection, including issues surrounding Cloud computing[136] in May of 2011. In the report, the OPC applauds that Bill C-29 includes breach notification measures. These measures have been considered inadequate by some notable academics[137] as lacking teeth. Industry, on the other hand, has approached breach notification cautiously, especially in terms of penalties for non-compliance,[138] and is generally of the view, as will be discussed in more detail below, that mandatory breach notification should not be part of a legislative scheme in Canada, or at least, that industry is allowed much discretion regarding when and whom to notify.

The Canadian OPC is currently amongst the leaders in the international data protection arena. A prominent recent example of this trailblazing was the Facebook case. It was in response to this inquiry that Facebook agreed to make changes to its

---

134 Jack Newton, "Clouded Thinking; Will regulator fear turn Canada into a cloud computing ghetto?", Slaw Blog, online: Slaw Blog www. slaw.ca.

135 Robert Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," World Privacy Forum (February 23, 2009), online: World Privacy Forum http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf as cited in Caught in the Clouds>, *supra* at 44.

136 See 2011 Report, *supra*.

137 Michael Geist, "The anti-privacy privacy Bill", Michael Geist Blog, online: Michael Geist Blog <http://www.michaelgeist.ca/content/view/5059/125/>.

138 Canadian Bankers' Association, "*S*ubmission by CBA to Industry Canada" (January 15, 2008) online: Canadian Bankers' Association www.cba.ca/contents /files/submissions/sub_20080117_01_en.pdf.

privacy policies and standards, which are, of course, in effect globally.[139] Among the changes brought about by the Commissioner related to sharing information with 3rd party applications only on *express* consent, clarifying rules on the deactivation of accounts and also the tracking of non-users who were invited to join Facebook, but declined to do so.

But the federal commissioner is not the only active player in Canada. Provincial Commissioners, like Frank Work in Alberta and, in particular Dr. Ann Cavoukian, the Ontario Information and Privacy Commissioner of ("IPC"), are also among those providing helpful insights and positions on privacy and its role in the Web 2.0 world. Dr. Cavoukian recently released a document which proposes a privacy-by-design model[140] as the central protection measure for privacy in the Cloud. In this model, the Commissioner promotes a six-principle approach, at the core of which lies encryption technology. In order to allow cloud technologies to develop while providing adequate protection for individuals' personal information it would be necessary to address the data protection concerns while allowing for adequate access to the data (or else the cloud model would not work). To ensure this, it is proposed that an audit architecture, along with a cloud identity service provider would be introduced into the individual-customer-CSP relationship.

The IPC has also published a white paper[141] on the Internet's implications on privacy, in which she promotes the use of privacy enhancing technologies (PETSs), which include elements called private "tokens",[142] bits of encrypted data to establish the identity of the individual *vis a vis* the ISP without actually revealing the identity of the individual. Criminal investigations would still be possible with these tokens because the token is *capable* of being traced back to the individual.The privacy-by-design model proposed by the IPC essentially advocates the architecture of all systems that process personal data to be designed so that they include privacy considerations at the outset, and not as an afterthought. This model has now gained international recognition and was adopted by the 32nd International Conference of Data Protection and Privacy Commissioners as a Resolution.[143]

With respect to lawful access, in particular the proposed legislation discussed

---

139 Press Release, "Facebook agrees to address Privacy Commissioner's concerns", Office of the Privacy Commissioner of Canada, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm>.

140 Information and Privacy Commissioner of Ontario and NEC Company, Ltd. "Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach" (May 2010) online: Information and Privacy Commissioner of Ontario www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf.

141 Dr. Ann Cavoukian, "Privacy in the Clouds", Information and Privacy Commissioner of Ontario, May 28, 2008, online: Information and Privacy Commissioner of Ontario www.ipc.on.ca/images/Resources/privacyintheclouds.pdf.

142 For more on these tokens, see the discussion of these in Code 2.0, *supra*.

143 Press Release, ""Privacy: Generations", the 32nd International Conference of Data Protection and Privacy Commissioners closes with a new executive committee and new members", 2nd International Conference of Data Protection and Privacy Commission–ers, online: Privacy Conference <http://privacyconference2010.org/news_view.asp?id=24>.

above, the OPC has voiced grave concerns[144] (at the time in regard to Bills C-46 and 47):

> In summary, we urge Parliament to review Bills C-46 and C-47 in light of the following questions: In specific terms, *how is the current regime of judicial authorization not meeting the needs of law enforcement and national security authorities in relation to the Internet*? What law enforcement or national security duty justifies *access without a warrant* by authorities to personal information or preservation of private communication? Why are some of these powers unrestricted, when the spirit of Canadian law clearly reflects the view that access or seizure without court authorization should be exceptional? And finally, are the mechanisms for accountability commensurate to the unprecedented powers envisaged (emphasis added)?

These concerns have been echoed and perhaps even escalated with respect to bills C-50, 51 and 52, and now C-30. The Ontario Commissioner has created an entire website devoted to raising awareness surrounding privacy invasive features of this tabled legislation.[145] 2012 will shed more light on whether the concerns of the OPC and IPC will bring about additional changes to the lawful interception proposals but the concerns stated above have been voiced since the beginning of the consultation period and have consistently related to the proposed legislation overstepping the privacy rights guaranteed by the *Charter of Rights and Freedoms*.[146]

(b) Europe

(i) Legislation

The European Union currently comprises 27 nations. Each one of these has its own distinct tradition with respect to the nature of how the term "privacy" (or the equivalent value in that tradition) is to be understood, as well as protected and regulated.[147] The basic data protection framework consists of the Data Protection Directive, the Directive on Privacy and Electronic Communications (e-privacy Directive),[148] the Data Retention Directive,[149] and the 2009 e-privacy Directive.[150]

The Data Protection Directive and the e-privacy Directive provide the general framework for data protection in Europe. One of the cornerstones of this framework is that personal data may not be transferred to a country that does not have

---

144 Jennifer Stoddart, "Letter regarding initial implications of Bill C-46 and Bill C-47", Office of the Privacy Commissioner of Canada, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/parl/2009/let_091027_e.cfm>.

145 Real Privacy, online: <http://www.realprivacy.ca/>.

146 See Justice Canada, "Comments by Canada's Privacy Commissioners", Justice Canada, online: Justice Canada <http://www.justice.gc.ca/eng/cons/la-al/sum-res/5.html>.

147 See Lee Bygrave, *supra*.

148 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002.

149 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006.

150 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

"adequate protection"[151] (as determined by the EU Commission). Data flows may not, on the other hand, be restricted within the EU on the grounds that data protection is inadequate.[152]

A note on the recently released proposal to amend the EU data protection framework: this paper was researched and written prior to the publishing of the EU proposal for a new privacy framework. The proposal's aim is to harmonize the EU landscape by implementing a directly effective Regulation (rather than guiding Directive), which is surely a step in the right direction for cloud proliferation. There are also steps to simplify the administrative process: for example, dealing with one DPA rather than one in every Member State to approve data transfers. However, this first proposal may do very little to assist cloud adoption outside of the EU. As the most evident example of this are the continued restrictions on data transfers as well as the requirement to obtain explicit opt-in consent for all processing of personal data, as well as strict data breach notification provisions, coupled with privacy-by-design obligations.[153] The fact that the most severe breaches can cost organizations up to two percent of annual turnover only increases the risk associated with the Cloud.[154] The expected date of a finalized piece of legislation is 2014.

(A) Trans-border Transfer

The European approach to data transfers is anchored in Article 25 of the Data Protection Directive, which prohibits the transfer of data into third countries without "adequate protection" for the data. Transfers are only permitted under: a) specific circumstances listed in Article 26(1), b) where the transferee organization has signed on to the Safe Harbor[155] agreement, or c) where the organization uses "binding corporate rules"[156] (when transferring between groups of companies or international organizations) or "EU Model Contract Clauses".[157] The *Article 29 Working Party*[158] has developed a number of policy documents for the use of organizations wishing to use "binding corporate rules" ("BCRs") as a workaround to Article 25.[159]

---

151 Article 25.

152 Data Protection Directive, Article 1(2).

153 EU Proposal, *supra*, Article 23.

154 *Ibid*.

155 See Export.Gov, online: <http://export.gov/safeharbor/eu/eg_main_018365.asp>.

156 European Commission, Data Protection Overview, online: European Commission <http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm>.

157 *Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council* (Feb. 5, 2010).

158 Established under Article 29 of the Data Protection Directive to fulfill the tasks listed in Article 30. These relate most prominently to advising the European Commission on data protection matters.

159 From glossary, European Data Protection Supervisor, online: European Data Protection Supvervisor, <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/72>; WP 107: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules" (pdf);

The most notable of these *inadequate* countries is the US. The reasons for this are rooted in the provisions of the *USA Patriot Act*, which gives broad surveillance powers to law enforcement. Whether or not the Safe Harbor agreement would trump US law such as the *USA Patriot Act*, is as of date legally uncertain. It follows then, that data transferred to the US might not necessarily be "safer" through Safe Harbor, at least not until this question has been raised and decided by American courts. This issue aside, many important CSPs are American, with data centres in the US and elsewhere. Some CSPs may have signed on to Safe Harbor but certainly not all providers will have done so. In these cases, European legislation is a bar to European customers using cloud services, where information in not only outsourced but often also to locations unknown to the customer (and the data subject). Germany's Commissioner makes the following relevant points here:

> With regard to data processing outside the EU, an adequate level of data protection must be ensured in any location to which data can be transferred in connection with CC. *Since the Cloud is not, however, geographically limited per definition, it is hard to imagine whether and how it is possible at all to put the requirements relating to data protection law into practice* (emphasis added).[160]

It is hard to imagine in this situation that a data subject *is* able to give his or her "consent" (as this is understood in Article 26(1)) to the transfer to a country without adequate protection. From a compliance perspective, lawful access by US officials via the *USA Patriot Act* may be a concern for potential cloud customers as well as regulators, but from a pure legal perspective this is less pressing than the concern that storing data outside of the EU runs afoul Article 25. Uploading data into the Cloud is considered "processing" under EU law[161] and so therefore the Data Protection Directive will apply to CSPs processing personal information of EU data subjects, whether or not the CSPs are based in the EU or not. On this point one must note, however, that according to the *Bodil Lindkvist*[162] case, uploading information onto a webpage is not to be considered a "transfer" of personal data within the meaning of Article 25 of the Directive. That is, the act of uploading a photo on Flickr without further processing would not come within the purview of the legislation.

The exceptions to the transfer prohibition, such as model contract clauses, although considered a good initiative, are by no means a complete answer to data transfer among customers and CSPs, as all parties must be under the *same* obliga-

---

WP 108: Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules (pdf); WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data; WP 153: Working Document setting a table with the elements and principles to be found in Binding Corporate Rules (pdf); WP 154: Working Document Setting up a framework for the structure of Binding Corporate Rules (pdf); WP 155: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules (pdf).

160 Peter Schaar's comments, *supra*.

161 Lanois, *supra* at 46.

162 (2004/C7/04).

tions (not just "similar" as under Canadian law). Implementing these will be a challenge in a cloud environment.[163] To address these challenges, CSPs have been offering "European Cloud" services that isolate European data from other data[164] but these measures will not be enough if the long-term goal is to have Europeans benefitting from the model to the full extent. That is, at some point, there must be clarity on the regulations affecting CSPs and cloud customers (if the goal is, of course, to advance cloud adoption). Sweden's DPA has recently released a document on the obligations of companies wanting to use CSPs but added little in way of practical guidance that would allow worry-free use of non-EU, in particular US, CSPs.[165]

(B) Data Intrusion

European law mandates Member States to include breach notification provisions for "providers of electronic communications services" in their national laws by May, 2011 by virtue of the 2009 e-privacy Directive. Article 4 in the e-Privacy Directive obliges Telecommunications companies to notify subscribers in case of the risk of a security breach regarding electronically stored personal data and the 2009 Directive expanded the framework to include breach notification provisions for all personal data:[166]

> In the case of a personal data breach,[167] the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to *adversely affect* the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay. Notification of a personal data breach to a subscriber or individual concerned *shall not be required* if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.
>
> The notification to the subscriber or individual shall *at least describe the*

163 See Lanois, *supra*.

164 See IBM Whitepaper, *supra*.

165 Swedish Data Inspection Board, "Cloud Services and the *Personal Data Act*", online: <http://www.datainspektionen.se/Documents/faktablad-cloudservices.pdf>: A Controller must "adopt a position regarding whether the cloud service provider may disclose personal data to a so-called third country, i.e. a country outside the EU/EEA and whether, in such a case, the transfer is supported by the *Personal Data Act*."

166 Article 3(c) adding (3) to Article 4 of the e-privacy Directive.

167 2009 e-Privacy Directive: "means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."

> *nature of the personal data breach* and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach (emphasis added).

Note that the threshold to notify is "adversely affect", which is rather broad and thus allows for less discretion on the part of the organization on whether or not to notify. This will naturally increase the control of the individual over their data because they will know not only of major breaches but of any that have an adverse affect. Should a company fall short of this notification requirement the competent authority "shall impose appropriate sanctions in the event of a failure to do so."[168]

Germany's *Datenschutzgesetz*[169] stipulates a mandatory breach notification procedure that requires breach notification where the breach was with respect to four categories of sensitive data.[170] The competent authority must be notified immediately in cases of "threats of serious harm or to the rights of legitimate interests of data subjects". Individuals must be informed of the breach, but only after "appropriate measures to safeguard the data have been taken and notification would no longer endanger criminal prosecution." The requirement is, unlike to the European framework, not limited to telecommunications providers and will apply to *all* data controllers.

Although not as fragmented as the data retention scheme, EU notification procedures differ from jurisdiction to jurisdiction. Since CSPs will many times be storing data from citizens from different member states, they will need to be aware of all local laws in order to be compliant, rather than being able to focus on one set of rules. The advantage of this scheme is that users of a cloud service in Europe can rest assured that breaches will be brought to their or to the authorities' attention, which may increase the comfort level of customers opting to choose cloud services. That is, there is no uncertainty from a citizen's perspective with respect to how they will be notified, at least by law, in case of a data breach. Industry, however, may have a considerable level of discomfort, knowing that they may be onside one but another set of laws, all within Europe and for the same service. Compared with the United States, this is not a significant disadvantage, as many states have their own, and quite divergent, set of privacy laws. Compared with jurisdictions that have a more uniform set of laws, including Canada, however, this will be a likely drawback for industry, where foreseeability and consistency is highly desirable.

(C) Lawful Access

Lawful access in the EU is governed by the Council Resolution on *Lawful*

---

168 Article 5(3) e-Privacy Directive.

169 §42a, BGBI. I S. 201, January 27, 1977.

170 BDSG §42 "special categories of personal data (Section 3 (9)), 2. personal data subject to professional secrecy,3. personal data referring to criminal or administrative offences or to suspected criminal or administrative offences, or4. personal data concerning bank or credit card accounts."

Interception of Telecommunications.[171] The powers granted to law enforcement are not significantly different from the Canadian framework and will therefore not be illustrated in more detail. What is highly relevant, however, is that European countries have taken a variety of different approaches on legal interception. One cannot speak of a harmonized framework at all.[172] Countries such as Sweden, Germany[173] and the United Kingdom[174] have passed legislation requiring Telecommunications companies, including ISPs, to enable lawful interception of telecommunications by law enforcement, but the requirements imposed on ISPs are not uniform from country to country.[175] For example, the legislation in Germany and the U.K. applies to IPSs with more than 10,000 subscribers, but unlike in the U.K., German IPSs are not entitled to compensation for costs incurred while complying with the legislation.[176] In Sweden, a highly controversial[177] "wire-tapping" law entered into force in October of 2009,[178] which some say goes much beyond the EU Directive in terms of access to data.

The Data Retention Directive places an additional burden on ISPs by requiring Member States to pass legislation to have IPSs retain traffic data,[179] such as email address and IP address, for a period of 6–24 months.[180] In fact, Member States may require periods exceeding 24 months. But again, not all Member States have translated the Directive into national law. European countries have taken different approaches in this regard. Sweden, for example, had initially refused to do so entirely[181] and has yet to implement the Directive (a proposal was tabled in November 2010 for a law to be in force by the middle of 2011). The proposal sets forth the minimum 6-month retention period on the one hand but proposes to include more data than the Directive demands.[182] Contrast this with Germany where

---

171 Council Resolution of January 17, 1005 (9529/95 ENFOPOL 90).

172 See Conny Larsson, "Telecom Companies as Crime Investigators", in *Scandinavian Studies in Law, Vol. 47* at 436.

173 *Verordnung über die technische und organisatorische Umsetzung von Maβnahmen zur Überwachung der Telekommunikation, (*BGBI. I. S. 458), January 22, 2002.

174 *Regulation of Investigatory Powers Act 2000* (c. 23).

175 *Swedish Act on Electronic Communications*, (1993:597).

176 Ian Lloyd, *Information Technology Law*, (OUP: Oxford, 2008) at 266, compare with Larsson, *supra* at 435.

177 See Wikipedia, "FRA-law", Wikipedia, online <http://en.wikipedia.org/wiki/FRA_law>.

178 The so-called "FRA-law", cited as *Proposition 2006/07:63 — En anpassad försvarsunderrättelseverksamhet*.

179 In the e-privacy Directive this means "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof".

180 Article 6.

181 See Mikael Ricknäs "Sweden Challenges EU Data Retention Directive", Computer World, online: Computer World <http://www.computerworld.com/s/article/9133566/Sweden_challenges_EU_data_retention_directive.

182 "Ask vill lagre mer an EU kraver", Dagens Nyheter, online at <http://www.dn.se/nyheter/politik/ask-vill-lagra-mer-data-an-eu-kraver>, last accessed

the German Federal Court held that national transposition of the Directive was inconsistent with the *Grundgesetz* (German Basic Law/Constitution).[183] This illustrates two of the biggest issues for European law in this respect: consistency and foreseeability.

With respect to the cloud computing model, lawful interception and data retention are obvious causes for concern in Europe. The lack of harmonization has a direct negative effect on CSPs (and customers), who may be unsure of their obligations, not to mention being subject to additional costs. On this point, privacy watchdogs and industry make for strange bedfellows. Industry players and data protection authorities may be at odds on a number of issues,[184] but here it is in both their interests to see data retention and legal interception harmonized or abolished.

(D) Jurisdiction

The Data Protection Directive will apply to all organizations established, or using equipment situated in the EU (or where Directive would apply on account of international law), who process personal data.[185] "Equipment" would include data and hosting servers, but could also include a personal computer or cookies where those are used to process personal data. This means, for example, that a non-EU resident private person who processes personal data while in the EU would be subject to the Directive.

European authorities have also taken the position that foreign organizations with entities within the European Union, must adapt their data protection policies to comply with EU Law.[186] In the SWIFT[187] decision it was ultimately held that SWIFT's US operations were not obliged to adhere to European law but this was only after SWIFT in the US joined Safe Harbor, and it does show that European authorities will assert jurisdiction over foreign entities. European authorities may also assert jurisdiction where information is transferred onward by a foreign entity. The European Commission has stated that an "onward transfer" must comply with

---

on January 12, 2011, whereby Minister Beatrice Ask petitions for the data to include information regarding unanswered phone calls as well as the location of those calls.

183 See e.g. Monika Ermert, "Court Finds German Data Retention Law Unconstitutional," IP Watch, online: IP Watch <http://www.ip-watch.org/weblog/2010/03/02/court-german-data-retention-law-unconstitutional>.

184 See, e.g. *Report of Findings: CIPPIC vs. Facebook Inc. under PIPEDA* (July 16, 2009) and the controversy surrounding Google's Street View and Buzz products, see e.g. "Letter to Eric Schmidt" (April 19, 2010), Office of the Privacy Commissioner of Canada, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm>.

185 Data Protection Directive, Article 4.

186 See discussion of the SWIFT case in "Data Protection Law and International Jurisdiction on the Internet", Int J Law Info Tech (2010) 18 (3): 227–247. *doi: 10.1093/ijlit/eaq004*. First published online March 11, 2010.

187 *Belgian Privacy Commission, Decision of 9 December 2008 in the SWIFT Affair*, unofficial English translation online: Privacy Commission <<http://www.privacycommission.be/en/static/pdf/cbpl-documents/a10268302-v1-0-151208_translation_recommswift_final.pdf>.

the principles of EU law.[188] Where personal data is transferred to a CSP with servers in multiple jurisdictions it is relatively clear that EU law will apply alongside the local law of the location of the servers. Where, for example, an American CSP receives personal data of European data subjects and wishes to transfer this data for further processing within the US, it must be aware of European laws and adhere to them. This may be cumbersome for CSPs but provides a certain degree of comfort to individuals who can rest assured that their personal data will receive a similar level of protection even after transferred into the geographical uncertainties of the Cloud.

(E) Status of CSPs

EU law differentiates between data "controllers", "processors" and "third parties".[189] Processors process data "on behalf" of the controller but their data protection responsibilities differ from those of the controller. Article 16 of the Data Protection Directive obliges the processor, or a person acting on her behalf, to only process data "on instruction" from the controller (unless required to do so by law). Article 17[190] outlines the duties of the controller *vis a vis* the processor and a review of these illustrates the importance of the distinction between the two terms. The controller, not the processor, carries the ultimate responsibility for the personal

188 See Data Protection Law, *supra*.

189 These terms are defined in the Data Protection Directive as follows: "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; "processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

190 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, *where processing is carried out on his behalf*, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, *and must ensure compliance with those measures*. 3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller,- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

data. In an Opinion in early 2010 the *Article 29 Working Party* clarified[191] the concepts of the respective duties of controller and processor, and then at the end of that year, it included CSPs in this clarification, at least to a certain extent. The user of the cloud service would be the data controller in most circumstances, but CSP may also be considered a data controller:

> If the cloud service provider uses means in the EU, it will be subject to EU data protection law on the basis of Article 4(1)c. As demonstrated below, the application of the Directive would not be triggered by means used for transit purposes only, but it would be triggered by more specific equipment e.g. if the service uses calculating facilities, runs java scripts or installs cookies with the purpose of storing and retrieving personal data of users. The cloud service provider will then have to provide users with information on the way data are being processed, stored, possibly accessed by third parties, and to guarantee appropriate security measures to protect the information.[192]

PIPEDA does not distinguish between a controller and processor in the same way as the Data Protection Directive, and so the ultimate outcome of this determination could (but need not) be that the same CSP is considered a "controller" under the EU law and but fall outside of the obligations of PIPEDA in Canada. A CSP may also be considered a "controller" by virtue of having "joint" control under Article 2(d) of the Directive. However, the joint control concept does not exist in all Member States, most notably Germany. This issue lack of certainty is a major concern for industry and potential customers and will need to be addressed in the upcoming years.

(ii) Government Cloud Strategies

The recently unveiled ICT strategy of Germany[193] along with the related "Cloud Computing: Aktionsprogramm"[194] indicates that Germany intends to be among the leaders within the G-8 and G-20 in this regard. The program and the overall strategy are explicit in its statement that the German Government wishes to "accelerate" the adoption of cloud computing in Germany, in particular the small and medium-sized business sector. In order to achieve this primary goal, four measures[195] are pinpointed; among them the establishment of workable legal solutions to cope with the novel issues the Cloud raises. BITKOM, Germany's IT industry

---

191 Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 169 adopted on January 16, 2010.

192 Opinion 8/2010 on applicable law, 0836-02/10/EN WP 179adopted on December 16, 2010.

193 IKT (ICT) Strategy of the German Government, "Deutschland Digital 2015", BMWi, November 2010.

194 Bundesministerium für Wirtschaft und Technologie, Aktionsprogramm — Cloud Computing", Bundesministerium für Wirtschaft und Technologie, online: BMWI www.bmwi.de/. . ./aktionsprogramm-cloud-computing,property=pdf, bereich=bmwi,sprache=de,rwb=true.pdf.

195 Also, to 1) drive innovation and market potential, 2) assist in international developments and 3) provide "orientation knowledge".

association, has welcomed this strategy, stating that "swift" action on behalf of industry and government is needed to ensure Germany's competitiveness in the Cloud arena.[196]

At a European level, strategies for Cloud computing were also unveiled and developed during 2010. The Expert Report[197] includes an analysis of Europe's positioning to take a leading role in cloud development. While identifying a number of strengths and weaknesses, no direct mention was made regarding either the strength or weakness of European privacy laws. While there is no official European cloud strategy, the EU Digital Agenda Commissioner, Neelie Kroes, promised this will be forthcoming in 2011.[198] At this point, it looks like this strategy will be unveiled in early 2012. The consultation to the European Commission closed on August 31, 2011:

> I am excited about the potential benefits of cloud computing to cut costs, improve services and open up new business opportunities. We need a well-defined cloud computing strategy to ensure that we make the best use of this potential. The input we are requesting from all interested parties is important to get it right.[199]

In terms of governments themselves moving services into the Cloud, Europe has not made significant strides. However, ENISA (European Network and Information Security Society) has just released a report[200] to advise and guide governmental agencies in their adoption of cloud computing and there are signs that so-called "G-Clouds" are a thing of the not-so-distant future.

(iii) Views of Data Protection Authorities

In an open letter posted on the German Commissioner's website, commenting on European laws to adequately deal with personal data in the Cloud, Peter Schaar questions the ability of the Cloud to comply with German and EU data protection laws:

> As an example (of the problematic of European legislation and the cloud) I would like to refer to the provisions in Sect. 11 BDSG on commissioned data processing. The order in writing must contain detailed provisions on the processing and protection of the data, and prior to data processing and regularly in the course of data processing, the principal has to make sure that the provisions are complied with. This requires that the principal knows in detail which of the data are processed at which location and under which

---

196 BITKOM, "Cloud — Aktionsprogramm", Press Release (October 5th, 2010), BITKOM, online: BITKOM <http://www.bitkom.org/65433_65412.aspx, last accessed January 20, 2011>.

197 *Supra*.

198 Neelie Kroes, "Towards a European Cloud Strategy" (January 1, 2011) eGov Monitor, online: eGove Monitor <http://www.egovmonitor.com/node/40544>.

199 Nellie Kroes quoted in Information Policy, online: <http://www.i-policy.org/2011/05/eu-commission-may-publish-standardised-cloud-computing-terms.html>.

200 ENISA, Security and Resilience, January 17, 2011, ENISA, online: ENISA <http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds>.

> conditions. *But how is this to be managed if free server capacities are selected only on an ad hoc basis* (emphasis added)?[201]

Also in Germany, the *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*[202] recently pointed out that the *Bundesdatenschutzgesetz* is currently unfit to properly regulate personal data processing which is both border-crossing and divided in terms of responsibility, as can be the case in cloud computing. The members of the Conference make a number of suggestions to amend the *Bundesdatenschutzgesetz* (and corresponding *Länder* laws). Firstly, the concept of the "verantwortliche Stelle" (responsible party) is to be brought firmly in line with the definition of "controller"[203] in the Directive. Secondly, where there is more than one responsible party, regulations should be dependent on the ability to influence the processing[204] as well as the interests in the data of each processing party ("interessengerechte Verteilung der Verantwortlichkeit"). These suggestions are intended to achieve responsibility and accountability of each party to the data processing, where, *inter alia*, cloud computing is used, and will enable continued responsibility of the transferring party (where the ability to influence the data transferee exists). Additionally, it was argued that where there is simultaneous processing by multiple parties, obligations should rest with all parties involved in the processing (i.e. joint controllership).

Recently, however, the German DPA provided more specific guidance regarding cloud computing.[205] The recommendations provided therein may not have been exactly what industry was hoping for but at least they provide some much needed guidance on what *not* to do when engaging the services of a CSP. For example, the DPA has stated that sensitive data may not be transferred to a US cloud service (other than with the express consent of the individual), and that any party using a cloud provider in the US, even within Safe Harbor, must verify that the US provider will agree to abide by EU compliance regulations.

The Swedish Data Inspection Board had preliminary concerns[206] related to the risk with transferring information across the Internet, data intrusion, encryption,

---

201 See Peter Schaar's Comments, *supra*.

202 Der Landesbeauftragte für den Datenschutz Baden-Württemberg, "Ein modernes Datenschutzrecht für das 21. Jahrhundert" (March 18, 2010), online: <http://Bund für Datenschutz www.bfdi.bund.de/cae/. . ./79DSKEckpunktepapier Broschuere.pdf>_at 19.

203 "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law."

204 Under Canadian laws, the term "data processing" does not exist in the same way. Instead, one speaks of the "use", "disclosure" or "collection" of data.

205 Hogan Lovell, Online <http://www.hldataprotection.com/2011/10/articles/international-eu-privacy/pending-revision-of-eu-directive-prompts-questions-about-safe-harbor/>.

206 As noted in e-mail correspondence with Ulrika Andersson, Legal adviser, The Swedish Data Inspection Board, on November 15, 2010.

how the controller can ensure that the processor, i.e. the CSP, actually implements the privacy measures the controller is ultimately responsible for but has recently released its views on the obligations of Cloud users. While this document does not do much in the way of simplifying CSP-use, it does provide some clarity that the Swedish DPA will put the onus on the controller who will always be the CSP user and it is he who must ensure that the Swedish Act is complied with, including ensuring all processor and sub-processor agreements are in-line with his processing instructions (in turn compliant with the legislation).[207]

At the EU level, Peter Hustinx recently commented[208] stated that there are four main areas of concern, which need to be addressed in the framework: a) Applicable law, including a new criterion such as "targeting", b) International data transfers, including streamlining the use of binding corporate rules and extending the responsibility of controllers, c) Accountability and "privacy by design" would give strong incentives to ensure that cloud computing services are privacy friendly, and if necessary even with some "privacy by default", and d) "processor" obligations where services are provided to individuals acting in a purely personal capacity.

(c) Industry Views and Proposals

> People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people [. . .] That social norm is just something that has evolved over time.[209]

Facebook CEO Mark Zuckerberg's comments caused quite a stir[210] within the privacy community at the beginning of 2010. Whether the commotion was warranted or if Mr. Zuckerberg's comments actually reflect popular society's development aside, they provide an example of an industry viewpoint on perceived privacy expectations in the Web 2.0 era: privacy will be diminished online but people might not care or at a minimum, values regarding what is considered as being "private" have changed.

Many well-known businesses are now cloud service providers. These include Amazon, Google, Sales Force, IBM and Microsoft, as well as of course Facebook, which are all placing much hope in the future of cloud technologies and the popular adoption thereof. In recent submission to the European Union, Microsoft explained its vision for industry and government action with respect to data protection in Europe.[211] This vision includes the right balance between government, consumer and industry action to enable "cloud ready" infrastructure, coherent legal framework in Europe, transparency about privacy and security by cloud providers, and security of the systems. Contrary to the thoughts of data protection authorities discussed

---

207 *Supra* note 157.

208 Peter Hustinx Speech, *supra*.

209 Mark Zuckerberg, as quoted in Bobbie Johnson, "Privacy no longer norm, says Facebook founder", The Guardian, online: The Guardian <http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy>.

210 See examples of this when entering the search terms privacy, social norm and Mark Zuckerberg into Google's search engine, last accessed on January 13, 2011.

211 Microsoft, "Building Confidence in the Cloud" (January 2010) online: Eurpean Commission ec.europa.eu/. . ./microsoft_corporation_2nd_document_en.pdf.

herein, industry does not share the same concerns that the cloud model is not *able* to comply with the current legal framework. Adjustments to the technical and legal frameworks may be called for but it would not be "impossible" to comply with a harmonized system and so that should be the primary legislative objective.[212]

In a "Joint Industry Statement on Data Protection" by the four major European Trade Associations of the Telecommunications Industry, it was pointed out that the European framework suffers from a lack of harmonization, unclear rules regarding the status of CSPs as processors and controllers, and a major barrier in the form of its restrictive trans-border data transfer policies.[213]

Microsoft also provided a response[214] to Canada's Digital Strategy consultation in which it both praised and criticized Canada's policies with respect to ICT. Among the criticism was that Canada was not "an early adopter" of ICT technologies and did not invest enough in digital technologies. With respect to privacy issues, Microsoft noted that Canada has a "robust" privacy regime but that PIPEDA needed to be overhauled. Bill C-29 was said to be a step in the right direction but may not be entirely sufficient. The paper went on to suggest that Canada needed a more comprehensive scheme for the transfer of data across borders but did not provide reasons for this view. This criticism is slightly unwarranted since the current Canadian scheme already addresses the transfer of personal data abroad and is quite clear about the obligations of the transferor, at least on paper.[215]

Compared with the consultation document to the European Union, at least with respect to data protection, Microsoft seems to be of the view that Canada has a more appropriate scheme at present. This may be less than surprising given that Canada is one, albeit large and diverse, country compared with the EU's 27 Member States, but noteworthy nonetheless. The current fragmented European Data Retention scheme was singled out as one of the most crucial impediments to widespread could adoption.[216] IBM has stated that a "lack of visibility and control, concerns about the protection of sensitive information and storage of regulated information in a shared, externally managed environment"[217] are major concerns and will be stopping wide-spread open cloud-computing solutions for a few years yet. For now, a "trust but verify" model is being promulgated by IBM. On the topic of breach notification, telecommunications providers such as Bell Canada have been

---

212 Roland Broch, "EuroCloud Deutschland schafft mehr Rechtssicherheit für Cloud Services", Eurocloud (March 3, 2010) online: Eurocloud <http://www.eurocloud.de/2010/03/03/eurocloud-deutschland-schafft-mehr-rechtssicherheit-fuer-cloud-services/#more-448>.

213 GSM Europe, "Joint Statement on Data Protection", GSM Europe, online: GSM Europe www.gsmeurope.org/. . ./Industry_*Joint*_Statement_on_Data_Protection.pdf

214 Microsoft Corporation, "Response to Canada DES Consultation" (July 2010), Government of Canada, online: Govnerment of Canada <http://de-en.gc.ca/home/>.

215 See OPC Guidelines, *supra*.

216 Building Confidence, *supra* at 4–10. Please note that industry has not made any official comments on Bill C-52.

217 IBM Whitepaper, *supra*.

outspoken in their views against mandatory regulations.[218] These views are shared by the Canadian Chamber of Commerce and relate to a fear of an over-flooding of notices (and resulting consumer fatigue in this respect).

Industry generally advocates that the current framework is not entirely incapable of handling privacy in cloud computing but needs to be harmonized and become clearer on the obligations of CSPs. New initiatives may also be needed and some of these are currently well on the way to becoming formulated.[219]

(d) Differences and Common Ground

As the preceding analysis has described, there are distinct differences but also common ground between Canada and the EU regarding data protection in the Cloud. This section will distill and analyze the main differences as well as the main points of commonality between Canada and the EU, and what these potentially entail for data protection in the Cloud.

Current legal frameworks are not suited to the Cloud: Neither the Canadian nor the European Union framework is currently able to properly address the challenges that the Cloud's inherent (and thus unalterable) features carry with them. Virtualization, and *ad hoc* data access and storage in multiple locations are not reconcilable with the Article 25 prohibition on the extra-EU transfer of personal data. They are also not easily reconciled with "openness" and "transparency" principles underlying PIPEDA. It will be difficult for a cloud customer to be open with respect to his practices *vis-a-vis* individuals, whose personal information she controls, if she does not know the CSPs, or their CSPs' practices (where multiple CSPs are used). The Directive's distinction between "controller" and "processor" may not be a feasible way in which to divide up responsibility for personal data in the Cloud and could result in uncertainty as to the ultimate responsibility for the data. The controller may not know about the CSPs practices at any given time because the services are delivered *ad hoc* but would still be "on the hook" for potential discrepancies. Bad for the customer, and possibly bad for the data subject's pri-

---

218 See comments made by David Elder, V.P. Regulatory Law, Bell Canada at *Standing committee on Access to Information, Privacy and Ethics*, 39th Parl. 2nd Session, January 1, 2007, Parliament of Canada, online: Parliament of Canada <http://www2.parl.gc.ca/HousePublications/Publication.aspx?

DocId=2654739&Language=E&Mode=1&Parl=39&Ses=1>.

"Instituting a duty to notify could create a more adversarial relationship between business and the OPC. In addition, imposing a *duty to notify on every potential breach could well do a disservice to the very consumers it is meant to protect*. This kind of requirement could result in a flood of notices being sent to consumers, desensitizing them to the gravity of a truly serious privacy breach. I believe we've seen this occurring in the U.S. Given this, the Canadian Chamber does not believe that mandatory breach notification is necessary in the legislation. We would encourage businesses to continue to work closely with the Privacy Commissioner's office in order to identify breaches and to notify those who could be affected by a possible breach in privacy. This flexibility enables notice where appropriate in the circumstances, with no adverse impact on consumers."

219 See for example, Digital Die Process Initiative as cited in Lanois, *supra*.

vacy, but good for the CSP. On the other hand, if CSPs were to be the "controller" of the data in a customer-CSP relationship (and not where individuals transact directly with the CSP or where the CSP acts outside of the initial processing relationship), too much of the responsibility would lie with them because the CSP does not have the relationship with the data subjects, including knowing, or being able to control, the purposes behind the collection of the data. At a minimum, however, both customer and CSP should be able to know into which category they fall. The Canadian OPC has offered some more guidance and how PIPEDA will apply to the CSP and the customer in its view, but the legislation itself is also not entirely clear on this point.

Government in the European Union and Canada is seeking more access to and control of personal data: The Canadian government is seeking to pass legislation to make lawful interception less cumbersome. The EU has passed data retention rules and countries within the EU already have means by which to legally intercept communications without a warrant. The most recent examples of these efforts are the FRA law in Sweden and the proposed legislation in Canada. This development is feared by both industry and data protection authorities, as well as by those concerned with the deterioration of data protection. As we have seen, threats to personal data by governments may still be the most serious threat to personal information, regardless of the amount of press the wanton privacy policies of Facebook or Google's invasive StreetView product have garnered. This continuing threat will be a deterrent for many businesses and individuals wanting to entrust their information into the Cloud because increased, even inadvertent, access may occur in the Cloud by way of these lawful access laws.

The Canadian legal framework is more "cloud-ready" than that of the EU: From the industry's perspective, it seems Canada has two distinct advantages regarding its governing legislation. Firstly, unlike the EU framework, PIPEDA allows for transfers to third countries via its organization-to-organization approach and secondly, its laws are much more harmonized internally as well as in relation to the United States (albeit with some well-established concerns about the US governments' lawful access provisions), both parties' most important trading partner in this respect.

The EU framework, although solid in its protection of personal information, is undoubtedly a roadblock for widespread cloud adoption in Europe, both on the customer uptake and the provider side. For one, the transfer restrictions do not work with the practical application of the public cloud application. Secondly, a lack of harmonization and resulting lack of foreseeability with respect to lawful access, data retention and breach notification requirements have industry worried about compliance where CSPs are situated in another Member State. Regulators and CSPs are attempting to come up with ways of negotiating around the transfer restrictions to non-adequate countries with agreements like Safe Harbor, BCRs and model contract clauses, but such a patch-work of a regulatory environment is not conducive to seamless adoption of a technology.

Canada need not worry about these same restrictions and can focus on the data protection issues from a more practical perspective. As an example, although the transparency and openness principles clash with the Cloud model, they are nonetheless principles that do not inherently clash with cloud computing if technological and business decisions are taken that incorporate privacy into the model itself. In

Canada, less of the discussion currently revolves around the *ability* of the legal framework to cope with the Cloud. Rather, both the Canadian and Ontario Commissioners are aiming at promoting technological solutions (privacy-by-design) and enforcing the laws *vis-a-vis* potential privacy outlaws (for example, Facebook and Google). The OPC has some concerns with the model and shares these with European counterparts but after an analysis of the material, it cannot be said that the worries are as far reaching as in Germany where, for example, the BDFI has voiced grave concerns with the model's ability to comply full-stop.[220] The Ontario Commissioner noted a related but lesser concern that if understanding, trust and assessment of the Cloud are not increased, the Cloud may be relegated to handling non-sensitive data,[221] rather than being an across-the-board option for data processing.

The Offices of the Canadian and Ontario Information and Privacy Commissioners are taking on a leading role in the quest for a data protective Cloud model: Canada has taken on a leadership role on the international data protection front, in particular with respect to digital data stored online. This is evident when looking at the shear level of activity of the OPC and IPC over the past two years, including investigating privacy breaches, writing open letter to industry, publishing material or making proposals at an international level.[222] Industry, privacy hawks and regulators all agree that this international cooperation will be crucial to the future of individuals' privacy rights online but also to the chances of the Cloud becoming a viable computing model for the future. Canada's leadership role may give potential cloud customers, including the government, the comfort level they require in order to trust their data to CSPs, even those in other countries. It will also provide comfort to those customers residing elsewhere that in case they trust a CSP with storage servers in Canada, their data will be protected by virtue of an active data protection authority. That being said, Canadian Privacy Commissioners recognize (or at least of the view) that laws will simply not do when it comes to data protection and the

---

220 Peter Schaar, *supra*, "In this connection, however, the question is raised how data protection and data security can be ensured. It is very hard to capture CC in its pure form — thus as an open, global model — by the applicable data protection law. If a data controller decides to have his personal data stored world-wide on dispersed computers, *this approach quickly reaches its limits*. In the extreme case neither the data subjects nor the data controller know where and by whom the data are technically processed. As far as storage capacities and applications (for instance text processing) are directly made available to the end users via the Web, the customers have hardly any chance to claim their data protection rights to which they are entitled to according to European law, at least in instances where the provider offers the service from a third country (for example the US). But also when domestic companies award orders related to data processing to providers of Cloud Services many questions are raised. Admittedly, the responsibility relating to data protection law normally remains with the data controller, thus with the principal. The *Federal Data Protection Act* (*BDSG*) and the European Data Protection Directive contain detailed provisions for such a case, however, as to CC (at least in its pure form), *it is hardly possible to comply with these provisions*."

221 Privacy by Design, *supra*, at 19.

222 See discussion infra and e.g. Cloud Computing & the Canadian Environment, *supra* at 4.

Cloud. What is needed are technological solutions and then laws as a supplement and enforcement tool.

Canadian and European laws continue to evolve alongside each other: All differences aside, Canadian and European legislation is more similar than not. In both cases, authorities will take jurisdiction where personal data of citizens and/or residents in being processed, both jurisdictions continue to pursue a more paternalistic approach to privacy, and both systems are very careful in terms of personal information being processed outside of their respective jurisdictions. Bill C-29 and the 2009 e-privacy Directive introducing breach notification requirements, is yet another example of a parallel development.

For industry it is obviously helpful to have similar requirements in their markets in case of wide-scale breaches where personal data from more than one region is compromised. In a cloud environment, a CSP may be hosting the information of data subjects from many different parts of the world, and compliance with non-harmonized and discrepant notification laws would be cumbersome to say the least. As we have seen, industry generally favours a self-regulating approach, but it seems that breach notification will become part of the general responsibilities of cloud providers, no matter where they are doing business. Bill C-29 strikes a balance between the call for mandatory breach notification and industry's wishes in that it neither allows for a private right of action nor does it impose clear penalties for non-compliance.

If Bill C-30 becomes a reality in Canada in some form or another, it will move Canada another step closer to (and perhaps even beyond) European legal interception laws, for better or for worse. From a privacy hawk's as well as industry's point of view, the data retention requirement is not a welcome development but would nonetheless be a step toward a more harmonized regulatory landscape, which is something industry is striving for.

So far Canada has a well-recognized and active data protection authority, which is leading the way on an international as well as domestic level. Canada's privacy laws strike a balance between the American and EU approaches as they are neither based on a self-regulating nor restrictive model of data protection (i.e. it permits data transfers but sets strict guidelines for doing so). Another advantage is that PIPEDA is considered to offer "adequate" protection under EU law. This allows a potential EU cloud customer to transfer personal data to a Canadian-based CSP without the fear of being offside Article 25 of the Directive.

The European Union Governments are farther along in the development of Cloud computing strategies:Both regions believe in the promise of the Cloud.[223] Both regions also seem to be confident in the benefits, both current and future, of pursuing a cloud-friendly regulatory environment, or, as in the case of the Canadian Privacy Commissioners and European Data Protection Authorities, technological solutions to ensure privacy in the Cloud. For businesses within the respective re-

---

223 In fact, there are not many voices opting for a "no-go" option. Even critics like Jonathan Zittrain, e.g. in Jonathan Zittrain, "Lost in the Cloud" (July 19, 2009) The New York Times, online: The New York Times<http://www.ny–times.com/2009/07/20/opinion/20zittrain.html> are not advocating to *not* use the Cloud model but just warning of its dangers and the need to develop and establish appropriate safeguards.

gions, it is seen as a way of cutting costs and achieving increased efficiencies. Not only that, both regions would like to viewed as feasible locations for CSPs to set up business, and where businesses (and consumers) would feel comfortable storing their personal data from an online privacy standpoint. However, Europe has a more well-defined and advocated cloud strategy. The Canadian government has been relatively slower (or cautious) in this respect. This wait-and-see approach has the advantage of avoiding hasty decisions from a data protection perspective but may prevent Canada from being at the forefront of developing appropriate data protection solutions even though it is regarded by many as being a prime location for the Cloud industry to prosper, especially in terms of constructing large-scale server parks in its Arctic North.

IV. FUTURE OUTLOOK

The Cloud promises many benefits but it carries with it many threats to personal information. Some of the threats come from hackers, others from industry's use, and others yet stem from the government's lawful access. All of these threats exist in the traditional environment but are exacerbated in the Cloud. Regulators, industry and data protection authorities have a major task ahead of them. They must make a square block fit a round hole. That is, the model that (almost) everyone seems to *want* to use must be reconciled with a framework that protects a fundamental right that is being threatened by that very technology. This reconciliation should also satisfy the competing rationalities referred to earlier. It is therefore not an easy task but one that could be achieved through choosing to follow along a number of different paths, some of which may be more desirable than others:

Option 1 would be that the Cloud model is more or less abandoned, used to a very limited extent or at the most used only where non-sensitive data is being transferred within private cloud applications. We have seen examples only to a limited extent but this is a concern that was voiced by Ontario's Commissioner. If there is no trust in the Cloud, then it unlikely that critical financial information or health or government records would be processed this way. Given the promise of the technology, however, this is an unlikely outcome.

Option 2 would be to reevaluate the values that stand in conflict with the model. In this case, regulators would engage in a simple cost-benefit analysis resulting in the conclusion that using the Cloud outweighs the harm caused to individuals' privacy rights and write laws so that the model can be used. There have been no proposals in this regard but as we have seen, certain comments from industry players have hinted that this should be considered.

Option 3 stops short of abandoning core values. Instead, it aims to rethink, reinterpret or add to current laws, without changing the underlying principles. This approach is evident in publications from the OPC and IPC, and targeted breach notification laws or policies clarifying the Article 25 prohibitions would be an example of this approach.

Lastly, *Option 4* would be to change the environment the technology is operating in so that the model suits the laws and values, and to write laws that encourage (or demand) use of that technology. This approach imagines the use of, for example, PETs and underlies, *inter alia*, the privacy-by-design approach advocated by the Ontario Commissioner. Given the realities of today's computing environment, it is perhaps the most promising way to satisfy privacy concerns as well as ensuring

the exploitation of new computing techniques.

2012 will likely provide us with an indication as to which options will be pursued and to what extent, in particular in response to the EU Proposal. Canada's privacy laws are also under review but, as noted, not as much progress has been made in 2011 as had been expected. Given that it is expected that the cloud computing industry will grow to $148.8 billion[224] by 2014, it naturally in many stakeholders' interests that clarity is provided swiftly.

CONCLUSION

Cloud computing is not a flavour-of-the-month technology and the protection of personal information is a core interest, notwithstanding a potential shift in what we consider to being "private" or how much information people are willing to share. The two concepts are clashing conceptually and in practice, and regulators, privacy watchdogs and industry are all grappling with how to reconcile an emerging, highly profitable technology with a fundamental right. Some believe that privacy and the Cloud are not at odds with each other *per se* but that it will require the re-thinking of how to protect privacy online and discovering and encouraging innovative technological solutions and architectures. Others, however, do not share this can-do attitude and hold the view that the model is inherently incompatible with the principles data protection laws were built upon. Others yet are of the view that the Cloud is the technological model of the future and that privacy ideals have changed so that current laws — and principles — need to be adjusted so that the benefits of the Cloud can be reaped.

We have seen that Canada and the European Union along with its Member States have many things in common with respect to the principles of the protection of personal data. This is also evident in the shared public wariness of warrantless government access to communications. Notwithstanding these similarities, the EU's size and lack of harmonization, restrictions on data transfers, controversial and inconsistently applied data retention and lawful access laws, make it quite a tough and uncertain legal landscape for CSPs and their potential customers. Reconciling privacy and cloud computing is also a challenge in Canada, but this process seems to be at least capable of being moved forward more effectively under the current legal and regulatory environment, although the Canadian Government's stalled digital strategy is putting this into question to a certain extent. 2012 will provide some answers whether this in fact will hold true and it will be very worthwhile for all stakeholders here to keep a close watch on the discussions ahead, in particular the views in response to the EU Proposal for a new EU data protection framework.

---

224 "Cloud to cause paradigm shift and transform businesses *KPMG report on 'The Cloud-Changing the Business Ecosystem*'", KPMG online: <http://www.kpmg.com/IN/en/Press%20Release/Press_Release_The_Cloud_Changing_the_Business_Ecosystem.pdf>.

Appendix 1 — List of Acronyms

BCR — Binding Corporate Rules
BDFI — German Data Protection Authority
CSP — Cloud Service Provider, provider of cloud computing services
DPA — Data Protection Authority
ENISA — European Network and Information Security Society
EU — European Union
IaaS — Infrastructure as a Service
ICT — Information and Communications Technology
ISP — Internet Service Provider
IPC — Information and Privacy Commissioner of Ontario
OPC — Office of the Privacy Commissioner of Canada
PaaS — Platform as a Service
PETs — Privacy enhancing technologies
PIPEDA — *Personal Information Protection and Electronics Documents Act*
SaaS — Software as a Service