CLOUD COMPUTING

A PRIVACY FAQ

In Canada, there is often a perception that using cloud computing services may be against the law or undermine privacy. This is often not the case. This FAQ guide will dispel some of the mythology around cloud computing and provide a framework to properly assess cloud computing and privacy.

By David Fraser

When contemplating a cloud computing solution, use your existing information system — warts and all — as the baseline from which you measure any potential decisions. As objectively as possible, you need to consider the security and privacy risks inherent in your corporate infrastructure.

Q Is it illegal for a Canadian business to outsource services such as cloud computing to a non-Canadian company?

A No. There is no law preventing most Canadian businesses from "exporting" personal information. Private-sector privacy laws require you to ensure a level of security for personal information comparable to that provided in Canada, regardless of whether you permit a Canadian or non-Canadian company to manage it. However, some highly regulated industries, such as banking, have special rules which may include additional regulation for outsourced services.

Q Is it illegal for a Canadian public sector or government body to outsource services such as cloud computing to a non-Canadian company?

A It depends on the jurisdiction of the public sector or government body. British Columbia and Nova Scotia are the only jurisdictions with laws strictly regulating the export of personal information from Canada by public bodies. For all other jurisdictions, including the federal jurisdiction, public sector bodies are permitted to export personal information, but must ensure a level of security comparable to that in Canada, regardless of whether a Canadian or non-Canadian company manages it. Alberta legislation makes it an offense for a public body or service provider to disclose personal information in response to an order with no jurisdiction in Alberta.

Q Is information better protected from law enforcement and national security access in Canada than in the United States?

A Not necessarily. The provisions of the *USA Patriot Act* that have attracted the most criticism have equivalents under Canadian law. Regardless of where information resides, it will always be subject to lawful disclosure to law enforcement or national security bodies. In Canada, this includes search warrants under the *Criminal Code of Canada* and the *Canadian Security Intelligence Service Act*, and administrative subpoenas such as those issued under the *Income Tax Act*. Many European countries permit broader law enforcement and national security access to information than either the United States or Canada permit.

Q Does keeping data in Canada keep it away from American law enforcement and national security agencies?

A In short, no. Canada, the United States and most Western democracies engage in a very high level of cooperation that includes mutual legal assistance treaties and ad hoc information sharing. In the area of "signals intelligence", Canada is a member of the "Five Eyes" program, under which Communications Surveillance Establishment Canada cooperates with the American National Security Agency, and their counterparts in the U.K., New Zealand and Australia. Most Canadian privacy laws actually permit this sort of information sharing under treaties or informal arrangements.

Q If we go with a cloud solution, should we give notify our customers/users?

A Under most Canadian laws, you technically do not need to seek consumer consent or provide notice. However, the Privacy Commissioner of Canada's position is that businesses proposing to have personal information processed outside of Canada should give customers notice. This is not required under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), but probably represents a best practice. Under the Alberta and Quebec private-sector privacy laws, you are required to give your customers notice.

Q What are the legal security requirements for Canadian companies considering cloud computing?

A Canadian legislation is silent about the particular security practices you should adopt when using cloud computing. PIPEDA, for example, only says that safeguards commensurate with the sensitivity of the information must be adopted: the more sensitive the information, the greater the precautions that should be taken. The general prevailing view is that you should insist on at least the industry best practices for the sort of data at issue.

The original organization remains legally responsible for safeguarding personal information even if it is outsourced. It is up to the organization to make sure that any service provider implements adequate protections.

You must be mindful of any additional risks cloud computing introduces. This is principally related to data being in transit over the open Internet. You can generally mitigate these risks by using SSL, VPN or other encryption technologies to make the information secure in transit. Provided you use a reputable provider, information is often safer when in the custody of a

> “AT A MINIMUM, YOU SHOULD **BE SURE** YOUR SERVICE PROVIDER IS BASED IN A JURISDICTION WITH A **MATURE AND FAIR** LEGAL SYSTEM.”

cloud service provider: cloud providers generally have greater resources to devote to security, and mobile users will no longer have to carry data with them in vulnerable devices such as laptops and USB drives.

Q What role should jurisdiction play in a decision about whether to adopt cloud computing?

A Jurisdiction is relevant but less so than most believe. For example, you should be very wary of any situation that casts doubt over whether your contract with your service provider will be enforceable. After all, their obligations to secure your data are set out in the contract. At a minimum, you should be sure your service provider is based in a jurisdiction with a mature and fair legal system. Data may fall under the jurisdiction of any country to which the service provider is reasonably connected. This includes, at minimum, where you are located, where the service provider is based and where the data resides. For each of these jurisdictions, consider whether it introduces any meaningful increase in risk to your data. It is very difficult to determine and measure this risk; you should seek expert legal advice to do so.

Q What should I look for in the contract with my service provider?

A Here are the top 10 things you should ask for. Not every service provider will negotiate these terms and, depending on the model of cloud computing the provider uses, some are simply difficult or impossible to deliver — but you should still ask for them and consider any response.

1. Limit the service provider to using your data for your purposes only, and for no other purpose unless you explicitly consent.

2. Include a provision that the service provider holds your data “in trust” for you, making it a legal fiduciary.

3. Prohibit the service provider from making any disclosures of your data without your consent, except as expressly set out in the agreement, and contemplate what it should do in response to a legal order for access.

4. Specify the damages to which you are entitled if the service provider discloses any data without your consent by using a multiplier connected to the extent of the disclosure, instead of a fixed sum, and characterized as general damages.

5. Obligate the service provider to resist — to the extent lawful and as soon as possible — orders to disclose information without your consent.

6. Obligate the service provider to cooperate with you in any regulators’ investigations.

7. Prohibit the service provider from dealing with any regulators related to your information without your participation.

8. Implement safeguards to protect information. Require that the service provider abide by accepted information security standards instead of constantly changing technologies — and that they be regularly audited against them by a third party, with access to the audit reports available to you. The provider should warrant it will do so and will cover your costs if there is a breach resulting from its lapse. Include your ability to audit your users’ access of the data.

9. Insist on full indemnity, without limitations, for liability related to privacy and security. The provider’s warranty and indemnity should cover all of your costs and any remedies you must offer your customers due to a security breach. Require the provider have and maintain adequate insurance for such incidents, and provide you with certificates of insurance.

10. Provide that you can get your data back and the service provider cannot retain or use it after the contract ends — and make sure you get all your data back!

Q What are the best practices for decision-making around cloud computing?

A As with any new program involving the handling of personal information, your organization should undertake a privacy impact assessment (PIA). PIAs are a systematic way of canvassing all of the privacy issues inherent in a project to identify — and hopefully mitigate — them. PIAs are widely done in the public sector; private sector organizations considering moving customer or employee data to a service provider should also conduct a PIA.

David Fraser, a partner with McInnes Cooper, is one of Canada’s leading internet, technology and privacy lawyers. He regularly advises a range of Canadian and international clients — from start-ups to Fortune 100 companies — on all aspects of technology and privacy laws, including cloud computing and PIAs. You can reach David at david.fraser@mcinnescooper.com or 902-444-8535, and follow his blog at blog.privacylawyer.ca. Visit McInnes Cooper at www.mcinnescooper.com.

L'INFONUAGIQUE

LA « FOIRE AUX QUESTIONS » SUR LE RESPECT DE LA VIE PRIVÉE

Q Est-il illégal pour une entreprise canadienne de sous-traiter des services tels que l'infonuagique à une société non canadienne?

R Non. Il n'existe pas de loi empêchant la plupart des entreprises canadiennes d'« exporter » les renseignements personnels. Les lois sur la protection des renseignements personnels applicables au secteur privé exigent d'assurer pour les renseignements personnels un degré de sécurité comparable à celui offert au Canada, peu importe qu'ils soient ou non confiés à une société canadienne. Toutefois, certaines industries fortement réglementées, telles que l'industrie bancaire, disposent de règles spécifiques pouvant inclure une réglementation supplémentaire pour les services sous-traités.

Q Est-il illégal pour un organisme du secteur public ou gouvernemental canadien de sous-traiter des services tels que l'infonuagique à une société non canadienne?

R Cela dépend de la province de l'organisme du secteur public ou gouvernemental. La Colombie-Britannique et la Nouvelle-Écosse sont les seules provinces qui ont adopté des lois réglementant strictement l'exportation des renseignements personnels du Canada par les agences publiques. Dans tous les autres ressorts, y compris le gouvernement fédéral, les organismes du secteur public sont autorisés à exporter les renseignements personnels, mais doivent fournir un degré de sécurité comparable à celui offert au Canada, peu importe que les renseignements personnels soient confiés à une société canadienne ou non. La législation de l'Alberta prévoit une infraction pour un organisme public ou un fournisseur de services qui divulgue des renseignements personnels en réponse à une ordonnance d'une autorité qui n'a pas compétence en Alberta.

Q Est-il obligatoire d'aviser les clients si l'on choisit de recourir à l'infonuagique?

R Dans la plupart des législations canadiennes, il n'est pas nécessaire en principe de solliciter le consentement du client ou de l'aviser. La position du Commissariat à la protection de la vie privée du Canada est cependant que les entreprises cherchant à faire traiter des renseignements personnels à l'extérieur du Canada devraient en informer leurs clients. Ceci n'est pas pour autant imposé par la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), mais constitue peut-être une meilleure pratique. Les lois de l'Alberta et du Québec sur la protection de la vie privée applicable au secteur privé prévoient l'obligation d'informer les clients.

Q Quelles sont les exigences légales de sécurité pour les entreprises canadiennes qui ont recours à l'infonuagique?

R La législation canadienne ne prévoit pas de disposition sur les pratiques particulières de sécurité que les entreprises devraient adoptées lorsqu'elles ont recours à l'infonuagique. Par exemple, la LPRPDE indique seulement que des mesures qui correspondent au niveau de confidentialité de l'information devraient être mises en place : plus le renseignement est sensible, plus grandes devraient être les précautions à prendre. L'idée générale qui prévaut est que l'on devrait insister, au moins, sur les meilleures pratiques de l'industrie concernant le genre de données en question.

L'organisme original demeure juridiquement responsable de la protection des renseignements personnels même lorsqu'ils sont sous-traités. Il appartient à celui-ci de veiller à ce que ses fournisseurs de services mettent en place des mesures de protection adéquates.

Il faut être au fait de l'évolution des risques dans le domaine de l'infonuagique. Cela concerne principalement les données qui transitent sur Internet. Il est généralement possible d'atténuer ces risques en utilisant SSL, VPN ou d'autres technologies de cryptage pour sécuriser les données en transit. Pourvu que vous choisissiez un fournisseur réputé, les renseignements sont souvent plus en sécurité lorsqu'ils sont conservés par un fournisseur de services en infonuagique : les fournisseurs en infonuagique disposent généralement plus de ressources à consacrer à la sécurité, ainsi les utilisateurs mobiles n'auront plus besoin d'emporter les données dans des appareils vulnérables tels que les ordinateurs portables ou les lecteurs USB.

Q Que devrait stipuler le contrat avec le fournisseur de services?

R Voici une liste des 10 principales stipulations que le contrat devrait comporter. Les fournisseurs de services n'accepteront pas tous de négocier ces modalités et, dépendant du modèle de services infonuagiques qu'ils utilisent, certaines d'entre elles sont simplement difficiles, voire impossibles à honorer — mais vous devriez tout de même les proposer et examiner toute réponse.

1. Limitez l'utilisation de vos données par le fournisseur de services à celle que vous désirez en faire, sauf autorisation contraire et expresse de votre part.

2. Incluez une clause selon laquelle le fournisseur de services détienne vos données « en fiducie » pour vous, faisant de lui un fiduciaire du point de vue juridique.

Suite à la page 40

de Winnipeg, dont le contentieux participe aussi au programme. Comme le contentieux s'occupe de toutes les affaires commerciales de la Ville de Winnipeg, cela permet aux étudiants d'apprendre beaucoup de choses. Le contentieux est à son tour satisfait du travail accompli par ceux-ci — avec les ressources limitées, toute aide est la bienvenue.

Mettre l'accent sur le mentorat et la diversité

Fernando Garcia, avocat principal chez Nissan Canada, est fermement convaincu de l'importance du mentorat. Il est mentor informel et membre du Comité de mentorat de l'ACCJE. Il fait remarquer que le Comité met davantage l'accent sur les moyens d'attirer les mentors et les mentorés de divers horizons. Selon lui, la diversité au sein de la profession juridique devrait être la pierre angulaire de tout projet.

Dans le même sens, *Legal Leaders for Diversity* (LLD), un groupe d'avocats généraux au Canada dont la mission est de faire respecter la diversité en milieu de travail, a lancé un programme de mentorat avec la Faculté de droit Osgoode Hall de l'Université York en 2012, s'ajoutant ainsi à d'autres programmes qui permettent aux étudiants de découvrir l'univers des juristes d'entreprise.

Devenir un partenaire stratégique

En ce qui concerne la formation des dirigeants, l'ACCJE a récemment lancé le Programme de leadership en entreprise pour les conseillers juridiques d'entreprises à l'issue duquel les diplômés reçoivent le titre de Juriste d'entreprise agréé – Canada (JEA.C). Les participants à la phase pilote considèrent le programme comme un pas en avant hors du commun dans la formation des juristes d'entreprise.

Pour ce qui est de l'avenir, Robert Lapper, chef de la direction du Barreau du Haut-Canada, pense que ce continuum de formations va s'enrichir et présenter des avantages pour les membres de la profession. Il précise que ce débat pourrait être pertinent pour les nombreux barreaux qui sont en train de réfléchir sur les structures d'entreprise alternatives pour l'exercice du droit.

C'est dans cette optique que le Projet de l'ABC Avenirs en Droit permet aux juristes de contribuer eux-mêmes à façonner l'avenir des services juridiques au Canada. Compte tenu des ramifications du changement sur le marché juridique et de ses répercussions sur l'exercice du droit, les membres de la profession doivent, ensemble, développer des stratégies et des outils pour aider les juristes, tant débutants que chevronnés, à réussir leur transition. ▮

L'INFONUAGIQUE : LA « FOIRE AUX QUESTIONS » SUR LE RESPECT DE LA VIE PRIVÉE *Suite de la page 37*

3. Interdisez au fournisseur de services de faire toute divulgation de vos données sans votre consentement, sauf mention expresse dans le contrat, et envisagez ce qu'il devrait faire advenant qu'une ordonnance lui intime de les divulguer.

4. Spécifiez les dommages-intérêts auxquels vous aurez droit si le fournisseur divulgue des renseignements sans votre autorisation, leur détermination étant faite en fonction d'un multiplicateur qui tient compte de l'ampleur de la divulgation et non selon une somme d'argent fixe, et leur qualification de dommages-intérêts généraux.

5. Obligez le fournisseur de services à ne pas exécuter les ordonnances de divulgation — dans la mesure permise par la loi et dès que possible — sans votre consentement.

6. Obligez le fournisseur de services à collaborer avec vous au cours d'enquêtes menées par des agences réglementaires.

7. Interdisez au fournisseur de services de traiter avec toute agence de réglementation en ce qui concerne vos informations sans votre participation.

8. Imposez des mesures de protection des renseignements. Exigez que le fournisseur respecte les normes de sécurité de l'information reconnues au lieu de changer constamment de technologie — et qu'elles fassent l'objet de vérifications régulières par une partie tierce, et enfin que vous ayez accès aux rapports de vérification. Le fournisseur devrait s'engager à couvrir vos frais en cas de manquement, de son fait. Ajoutez votre pouvoir d'effectuer la vérification de l'accès aux données par vos usagers.

9. Insistez sur l'indemnisation entière, sans limites, en matière de responsabilité liée à la protection de la vie privée et à la sécurité. Le contrat devrait stipuler sous les rubriques « Garantie » et « Indemnisation » que le fournisseur s'engage à couvrir vos frais et tous les dédommagements que vous devrez verser à vos clients en raison d'une faille dans la sécurité. Exigez du fournisseur qu'il possède des couvertures d'assurance adéquates pour ce genre d'incidents et qu'il vous remette les certificats d'assurance.

10. Indiquez que le fournisseur de service doit vous rendre vos données et qu'il ne peut pas les garder ou en faire usage après la clôture du contrat — et assurez-vous de retrouver toutes vos données! ▮