

Internet and E-Commerce Law in Canada

**Editor-in-Chief: Professor Michael A. Geist, Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law**

VOLUME 10, NUMBER 9

Cited as (2009-10) 10 I.E.C.L.C.

JANUARY 2010

• PEERING THROUGH THE CLOUD CLOUD COMPUTING: MANY BENEFITS BUT THERE ARE SOME LEGAL ISSUES TO CONSIDER •

Brad Newman
Business Law Group, Ogilvy Renault LLP

While outsourcing the processing or hosting of information is not a new idea, as many companies are familiar with application service providers (“ASPs”) and software-as-a-service (“SaaS”), “cloud computing” has become a catch-all phrase that represents the plethora of hosting and processing services available and delivered over the Internet.¹ The growing popularity with consumers of online services as well as the entrance of some brand-name vendors with corporate offerings (such as Amazon’s Elastic Compute Cloud (“EC2”), Google Apps and Micro-

soft’s recent announcement that Office 2010 will be offered as a free online service), has brought increased awareness to this combination of grid and utility computing services.² One study found that 69 per cent of Americans who use the Internet use some form of cloud computing, such as Hotmail and Gmail or online personal photo storage services.³

Cloud computing can be used by corporate clients to outsource, for example, data processing (such as massive database management or data mining), help desk management, CRM, word processing requirements and even all or a substantial portion of a company’s IT infrastructure. Many of the above, when implemented in-house, require expensive infrastructure that are often not used at maximum efficiency. One flavour of cloud computing that may be particularly attractive to businesses engaged in sensitive industries or handling sensitive information is the “Private Cloud”, whereby a business or other organization creates its own Internet-based data centre that is not generally available to the public.

With vastly improved features, usability and awareness, corporations and individuals are finding the siren call of cloud computing particularly compelling. While the benefits are many, the potential legal pitfalls that come with cloud computing must be considered.

First, some of the advantages that cloud computing offers:

• In This Issue •

PEERING THROUGH THE CLOUD
CLOUD COMPUTING: MANY BENEFITS BUT THERE ARE
SOME LEGAL ISSUES TO CONSIDER

Brad Newman.....81

HE SAID, SHE SAID: A WORLDVIEW ON
THE CHALLENGES OF CITIZEN JOURNALISM
AND PROVING DEFAMATION ONLINE

David Wotherspoon and Christian Leblanc.....85



INTERNET AND E-COMMERCE LAW IN CANADA

Internet and E-Commerce Law in Canada is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ontario L3T 7W8

© LexisNexis Canada Inc. 2009

All rights reserved. No part of this publication may be reproduced or stored in any material form (including photocopying or storing it in any medium by electronic means and whether or not transiently or incidentally to some other use of this publication) without the written permission of the copyright holder except in accordance with the provisions of the *Copyright Act*.

ISBN: 0-433-42472-9 ISSN 1494-4146
 ISBN: 0-433-44385-5 (print & PDF)
 ISBN: 0-433-44674-9 (PDF)

Subscription rates: \$190 plus GST per year (print or PDF)
 \$285 plus GST per year (print & PDF)

Please address all editorial inquiries to:

Boris Roginsky, Journals Editor
 LexisNexis Canada Inc.
 Tel. (905) 479-2665; Toll-Free Tel. 1-800-668-6481
 Fax (905) 479-2826; Toll-Free Fax 1-800-461-3275
 Internet e-mail: ieclc@lexisnexis.ca.

EDITORIAL BOARD

EDITOR-IN-CHIEF

Michael A. Geist, LL.B., LL.M., J.S.D., Canada Research Chair in Internet and E-Commerce Law, University of Ottawa, Faculty of Law, Ottawa

ADVISORY BOARD MEMBERS

- **Peter Ferguson**, Industry Canada, Ottawa
- **Bradley J. Freedman**, Borden Ladner Gervais, Vancouver
- **John D. Gregory**, Ministry of the Attorney General, Toronto
- **Dr. Sunny Handa**, Blake Cassels & Graydon, Montréal
- **Mark S. Hayes**, Hayes eLaw LLP, Toronto
- **Ian R. Kerr**, University of Ottawa, Faculty of Law, Ottawa
- **Cindy McGann**, Halogen Software Inc., Kanata
- **Suzanne Morin**, Bell Canada, Ottawa
- **Roger Tassé**, Gowling Lafleur Henderson, Ottawa.

Note: This newsletter solicits manuscripts for consideration by the Editor-in-Chief, who reserves the right to reject any manuscript or to publish it in revised form. The articles included in *Internet and E-Commerce Law in Canada* reflect the views of the individual authors. This newsletter is not intended to provide legal or other professional advice and readers should not act on the information contained in this newsletter without seeking specific independent advice on the particular matters with which they are concerned.



- **Pricing:** Some cloud providers' pricing models contemplate a monthly subscription fee while other vendors provide the services on a pay-as-you-go, utility-based model. For example, users pay for the volume of data stored or number of servers required.
- **Scalability:** Cloud vendors often allocate resources to a user as needed (or requested), which has obvious benefits for both the cloud vendor and user: cloud vendors benefit greatly from economies of scale and the efficient use of their resources, while users benefit from the resulting flow-through cost savings as well as the availability, often on-demand in real-time, of vast and flexible resources that can suit their needs without having to worry about whether too much or too little was spent on in-house IT deployments.
- **Transparency:** Users can typically see exactly how much they pay for their usage of specific services, whereas non-cloud vendors are often unwilling or unable to disclose how much a user is paying for each server used or gigabyte transferred.
- **Simple purchasing:** Though also a potential pitfall, many cloud computing services can be purchased over the Internet with a credit card and the services become available instantly. There is no need to issue a complicated request for proposal, but no opportunity to negotiate the terms of service.
- **Sensitive Data:** For businesses whose employees travel frequently and use portable laptops, the risk of loss, theft or confiscation of sensitive information stored locally on these devices can be mitigated, to some extent, by using cloud applications and storing data in the cloud.

However, all that glitters may not be gold. Companies must tread carefully when considering cloud computing as there are a variety of potential legal issues that need to be considered before engaging a cloud computing vendor:

- **Privacy:** Certain jurisdictions require personal information to remain within

that jurisdiction's borders unless the receiving jurisdiction has comparable legal safeguards. For example, the EU Data Protection Directive only permits the transfer of personal data to non-EU nations that ensure an "adequate level of protection".⁴ Cloud computing architecture, by its nature, provides that vendors may process resources in or through a number of jurisdictions at any given time. While in certain circumstances the cloud vendor can offer to limit where a specific user's data is held, it may not be possible or practical. Users also need to consider the risk that their data may be disclosed to the government of the jurisdiction in which their data is held by the vendor, possibly without their knowledge or consent. For example, the *USA PATRIOT Act* permits the U.S. federal government to seek a court order for disclosure of electronic records, often without permitting notice to the user.⁵ From a Canadian perspective, a company thinking about outsourcing the processing or storage of personal information to a cloud vendor needs to consider applicable legislation (such as the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("*PIPEDA*")), which may require:

- a) notice to the data subjects their information might be stored outside of Canada and their information may be accessed by governmental authorities according to the laws of that jurisdiction;⁶ and
- b) contractual obligations for the cloud vendor to safeguard personal information to the same extent as the company using the cloud services.⁷

Special considerations will apply if the prospective outsourcer is a federally regulated entity and therefore would have to comply with OSFI guidelines. The OSFI guidelines specify, among other things, that an outsourcing agreement is expected to point to a physical location where the outsourced activities are to take place; this requirement could make (non-private) cloud computing impractical.⁸ Additionally, the federal *Bank Act*, requires that certain records be stored in Canada.⁹

- **Foreign Governments:** The autonomy of private or state-sponsored enterprises varies between jurisdictions. It is important for the user to conduct due diligence and, if doubts persist about the potential for governments to monitor or access the user's systems or information flow, be sure to insist on appropriate confidentiality, security and indemnification protections or consider seeking an alternate cloud vendor.
- **Export Controls:** Given the multitude of locations from which cloud services may be provided by any one vendor, ensuring compliance with federal export controls may be difficult (where, for example, a company has sourced a software development platform in the cloud and the software to be developed contains encryption technologies subject to export controls).
- **Ownership:** Care has to be taken to ensure cloud vendor and user rights in their respective intellectual property are clearly delineated. For example, many cloud services involve the provision of proprietary development tools by the vendor, which allows the user to create its own databases, software or other applications. In order to ensure that the user comes away with a product that can be utilized by or licensed to other parties, it is essential to determine to what extent vendor or other third-party components are incorporated. Similarly, where mission critical or enterprise business processes are involved, it is critical to make certain that appropriate business continuity plans and possibly source code escrow agreements are in place to anticipate a potential bankruptcy of the vendor or some other cessation of the vendor's services.

As well, cloud vendor standard form contracts are often drafted decidedly in the cloud vendor's favour. Whether cloud computing is sourced for simple data processing or for enterprise resource planning for mission critical business processes, close attention should be paid to the following provisions commonly found in such standard form contracts — par-

ticularly if the services are going to be purchased online without any negotiation (also known as “off-the-shelf” services):

- **Uptime:** In July 2008, Amazon’s S3 experienced an outage lasting more than seven hours that affected all U.S. customers, including the high-profile social networking site Twitter.¹⁰ While some cloud vendors will include representations of high-levels of uptime backed by service credits issued in the event of outages (such as Amazon), others provide representations of nearly guaranteed uptime while also disclaiming liability for unanticipated or unscheduled delays or outages. Where the vendor is unwilling to negotiate, users should have their own back-up systems and business continuity plans in place to address possible long-term outages by key vendors, which should contemplate redundant data storage and backup services.
- **Security:** In July 2009, a hacker gained access to confidential documents stored on Google Apps by hacking a Twitter employee’s official email account — which was hosted by Gmail.¹¹ While it should be noted that access was apparently gained by the hacker as a result of poor password selection and protection by the victim, the incident serves as a reminder that sensitive information in the cloud can be vulnerable. Since vendors may not be forthcoming about their security measures and limitations of liability, in their standard form contracts, are often limited to the amount paid by the user or less, users may be out of luck if they suffer damages as a result of the loss or inadvertent disclosure of personal or sensitive information, or in the event of a security breach of the vendor’s systems.
- **Monitoring:** Many cloud vendors’ standard form contracts include the right to monitor all data which, without the inclusion of appropriate confidentiality and indemnification provisions, should be a source of concern for users who wish to

process sensitive business information in the cloud.

- **Varying Terms:** Another common inclusion in cloud vendor standard form contracts is the ability of the vendor to modify the terms of the agreement, with such modifications deemed accepted by either continued use any time after the new terms have been posted on the vendor’s website or after a certain stated time (*e.g.* 15 days after posting). An example of this is Apple Inc.’s recent modifications to the Terms of Service for its online service MobileMe. The notice provisions of the Terms of Service provide that notice of a change in the Terms of Service may be e-mailed, sent by regular mail *or posted on its website*. Apple recently added provisions related to its collection and use of customer information as well as adding a limitation of liability for any permanent cessation of the service.¹² If Apple chose to only post these important changes to its website, they would only be noticed if the customer visited the MobileMe website, yet the changes would likely have legal effect.
- **Pay the Bills:** The services agreement of one popular cloud vendor provides, in the event a user’s account falls into arrears, the vendor has the right to terminate and suspend access to the services. Perhaps most importantly, the vendor has no obligation to retain such user’s data, which may be “irretrievably deleted” after 30 days.

From this brief review of just some of the potential privacy issues in cloud computing, it is apparent that companies may encounter turbulence along the way.

CONCLUSION

The expanding and increasingly competitive marketplace of Internet-based outsourcing services that comprise the “cloud computing” lexicon provides vendors and users with lower overall costs of implementation thanks to economies of scale and greater scalability. However, both parties must be careful to ensure their interests are protected when entering into cloud computing arrangements, par-

ticularly those users purchasing off-the-shelf services subject to standard form contracts.

[*Editor's note:* Given the rapid developments in the field of cloud computing, please note that the article was originally authored in November 2009.

Brad Newman is an associate in Ogilvy Renault's Business Law Group in Toronto. His practice covers all aspects of corporate and commercial law, with an emphasis on IT-related matters. He can be reached at <bnewman@ogilvyrenault.com>.]

- ¹ For an overview of various cloud computing terminology and non-legal issues, see The Economist, "Special Report: Let it rise" (October 23, 2008), online: <http://www.economist.com/specialreports/displayStory.cfm?story_id=12411882>.
- ² Grid computing is the use of clusters of computers on a large scale to perform tasks that involve significant amounts of data and/or computer resources, while utility computing refers to the packaging of computing resources as a metered service.
- ³ John B. Horrigan, "Cloud Computing Gains in Currency" *Pew Research Center*, online: <<http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency>>.
- ⁴ See Council Directive 1995/46/EC at Article 25, online: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>>.

- ⁵ See Robert Gellman, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing (February 23, 2009): World Privacy Forum, online: <http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf>.
- ⁶ See Privacy Commissioner of Canada, "Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers" (PIPEDA Case Summary #2008-394), online: <http://www.priv.gc.ca/cf-dc/2008/394_20080807_e.cfm>.
- ⁷ See Privacy Commissioner of Canada, "Canadian-based company shares customer personal information with U.S. parent (Case Summary #2006-333)", online: <http://www.priv.gc.ca/cf-dc/2006/333_20060511_e.cfm>.
- ⁸ See Office of the Superintendent of Financial Institutions, "Guideline B-10: Outsourcing of Business Activities, Functions and Processes" (March 2009), online: <http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/b10_e.pdf> at subpara. 7.2.1(a).
- ⁹ See, e.g., *Bank Act*, S.C. 1991, c. 46 at s. 239, which requires certain records to be kept at the head office of the bank or at such other place in Canada as the directors see fit [emphasis added].
- ¹⁰ CenterNetworks, "Amazon S3 Down" (July 20, 2008), online: <<http://www.centernetworks.com/amazon-s3-down-july-2008>>.
- ¹¹ Computerworld, "Twitter breach revives security issues with cloud computing" (July 27, 2009), online: <http://www.computerworld.com/s/article/9135893/Twitter_breach_revives_security_issues_with_cloud_computing>.
- ¹² TOSBack, "Apple MobileMe Terms of Service" (June 18, 2009), online: <<http://www.tosback.org/diff.php?vid=495>>.

• HE SAID, SHE SAID: A WORLDVIEW ON THE CHALLENGES OF CITIZEN JOURNALISM AND PROVING DEFAMATION ONLINE •

David Wotherspoon and Christian Leblanc
Fasken Martineau DuMoulin LLP

The phenomenon of citizen journalism — also known as grassroots media, people's media, participatory media, open source journalism and do-it-yourself journalism — is gaining momentum and prestige.

Citizen journalism is not exactly a new concept. Leaflets and community newsletters have long provided ordinary people with an outlet for their point of view. But the Internet has empowered citizen journalists with unprecedented access to a global audience and a new level of permanence to their comments.

In one sense, a citizen journalist today is anyone with access to the Internet and an interest in telling a story. Savvy bloggers have the technological tools to

compete with traditional journalists and media outlets on breaking news stories. Simple publishing software, handy mobile devices, and ubiquitous wireless connections are empowering ordinary people to actively create and disseminate news online.

The distinction between professional and citizen journalists is becoming blurred. Many professional journalists now publish their own professional and personal blogs. Meanwhile traditional news media are engaging citizens to provide reports — sometimes for a fee. And hybrid news sites, such as <OhMyNews.com>, use professional and citizen journalists equally to handle similar assignments.

Even the New York Times has launched citizen journalism sites for communities in and around New York City, and <CNN.com> has long featured contributions from citizen journalists, particularly homemade news videos.

But do these citizen journalists have the same obligations — and protections — as traditional media outlets? Given the global reach and permanence of Internet communications, citizen journalism is raising the stakes for the “responsible journalism” defense in defamation law suits.

Because of the international nature of citizen journalism, it’s also useful to take a broader world-view of the topic, keeping in mind some of the case-law in and outside the U.S. to understand how different countries view defamation on the internet. Here, we’ve taken a look at three core issues of citizen journalism — jurisdiction, accountability and “responsible journalism” — and how they have variously been addressed by countries in the English-speaking Western world, where we see a great deal of overlap in news coverage.

CROSS-JURISDICTIONAL CLAIMS

Given the global reach of the Internet, what law applies when confronting defamation? Before launching a case, a claimant must establish jurisdiction.

But establishing jurisdiction can often prove quite difficult, as it was in the seminal case *Braintech, Inc. v. Kostiuk*. The company Braintech had, in 1997, obtained a default judgment of \$300,000 for libel and disparagement claims after the defendant had posted defamatory material to an Internet message board.

However, the Supreme Court of British Columbia later determined the defendant’s only connection with the jurisdiction, in this case Texas, was a passive posting on an Internet bulletin board. Braintech attempted to enforce the default judgment against Kostiuk in British Columbia. Notably, there was no evidence of publication to any person in Texas, nor was there any evidence that Kostiuk had a business interest of any kind in Texas. The court held that:

... the complainant must offer better proof that the defendant has entered Texas than the mere possibility that someone in that jurisdiction might have reached out to cyberspace to bring the defamatory material to a screen in Texas ...¹

It would create a crippling effect on freedom of expression if, in every jurisdiction the world over in

which access to Internet could be achieved, a person who posts fair comment on a bulletin board could be haled before the courts of each of those countries where access to this bulletin could be obtained.

Online communications are not available in comprehensible form until downloaded onto a computer. Therefore, establishing jurisdiction hinges on proving where a person downloads the material and where damage to reputation is done.

This point was explored in the Australian case of *Dow Jones & Company Inc. v. Gutnick*. Dow Jones hosted an online magazine that published an article containing allegedly defamatory references to the plaintiff. The plaintiff was successful by narrowing the scope of his claim to allege that the damage suffered to his reputation occurred in Australia as a consequence of publication of the defamatory article in Australia.

Similarly in the Canadian case *Burke v. NYP Holdings*,² the plaintiff alleged that a column published in the New York Post and posted on the newspaper’s website (maintained by the newspaper and available globally) contained defamatory content. Ultimately, the British Columbia Supreme Court assumed jurisdiction over the matter finding that the tort occurred when the column was accessed from within British Columbia.

HOW FAR DOES ACCOUNTABILITY EXTEND?

Sorting out the source of a comment — and its credibility — is increasingly difficult online. In the faceless world of micro-blogging sites, fake celebrities can tarnish the reputation of their targets in just 140-character messages. Yet the anonymity (or false identity) offered by the Internet is only one challenge in holding people accountable for their postings. Even when the author discloses his or her name, how are readers to determine if the statements are objective or accurate? Who qualifies as a journalist today? And what are their responsibilities and protections when reporting?

So far the relatively new “responsible journalism defense” has only been contemplated in the context of traditional media and journalism: professional, paid, accredited journalists and official news agencies.

Defamation is an offense. But a journalist in some jurisdictions can escape liability by arguing a comment falls under one of several legal defenses: truth or justification, fair comment, jest, statutory immunity, privilege, or responsible journalism. This last defense — responsible journalism — was first used

successfully in England in 1999 in the case of *Reynolds v. Times Newspapers*.³

The plaintiff, a former prime minister of Ireland, sued over a newspaper article that he interpreted as accusing him of intentionally misleading the legislature and lying to his colleagues. In its decision, the House of Lords considered three competing values:

1. the right of the public to access information on matters of legitimate public interest;
2. the ability of the press to report on such matters in a fair and responsible manner;
3. the protection of reputation.

In rendering the decision, Lord Nicholls said:

... the common law has recognized there are occasions when the public interest requires that publication to the world at large should be privileged. ... The court is concerned to assess whether the information was of sufficient value to the public that, in the public interest, it should be protected by privilege in the absence of malice.

And so the defense of responsible journalism was born. This landmark made valid the media's claim that — in some instances — it has a duty to publish an allegation even if it later turns out to be wrong.

The "Reynolds defense" was subsequently refined by the court in *Jameel (Mohammed) v. Wall Street Journal Europe*. The case concerned a report that the Saudi Arabian Monetary Authority was monitoring bank accounts associated with prominent businessmen to ensure they would not be used to transmit funds to terrorist organizations. The plaintiffs were among those named as under observation. In its ruling in favour of the media, the court provided for an increased freedom of the press as long as the media acts responsibly and in the public interest.

Some courts have relied on codes of ethics set by professional journalists' associations and on internal codes of ethics of media organizations. Traditionally truth has been the best defense of all in defending against claims of defamation.

DOES RESPONSIBLE JOURNALISM APPLY TO CITIZEN JOURNALISTS?

Can the responsible journalism defense apply equally to citizen journalists who run afoul of their subjects? There appears to be nothing, *per se*, that precludes applying the elements of responsible journalism to professional and citizen journalists alike.

Perhaps it is merely a matter of assessing what is reasonable for a given journalist in a given context.

Looking at the deep pockets of Internet Service Providers ("ISPs"), plaintiffs have attempted to name ISPs as defendants in defamation actions. They argue that ISPs share some characteristics with more traditional publishers — namely, the ability to edit content. But not all ISPs provide the same services. Some act solely as an access provider, connecting subscribing users with the Internet. Others provide email addresses, host content or host websites.

The law in other jurisdictions — particularly the United States and England — is inconsistent. To avoid a plea of innocent dissemination in the United States, the plaintiff must prove that the publisher was not innocent. Conversely, England does not presume innocent dissemination. Instead, the defendant publisher must establish its innocence to stand on this defense.

To date, Canadian jurisprudence does not speak directly to the liability of ISPs. Regardless of the services offered, ISPs are unlikely to act like newspaper editors so the law of innocent dissemination becomes relevant.

What does this theoretical risk mean in the real world? Consider a company contemplating using Web 2.0 to create an intranet site where employees can post comments. At first blush, it may seem prudent to install software to screen out obscene language. But if an employee then uses the site to make defamatory comments about a co-worker, the company may be held responsible as an editor. This same scenario could equally apply to media websites that allow members of the public to post comments online. The risk may be even greater for news aggregation sites such as the Drudge Report and Huffington Post that collect and republish links to stories and columns from other sources.

For true ISPs who merely provide the hardware and network connection for websites, there seems to be little risk of being caught up in defamation suits. But the minute someone exercises any form of control, there is a tendency for the courts to interpret that behaviour as editorial control.

It would be foolhardy to underestimate the power of online communications today — and in future. Individuals, institutions and companies alike continue to flock to the Internet because of the connection it offers to a potentially vast global audience. But the anonymity, immediacy, informality and per-

vasiveness of online communications make it an ideal breeding ground for defamatory statements.

[*Editor's Note:* In the light of the recent Supreme Court of Canada decisions, please note that the article was originally authored in September, 2009, and stay tuned for the detailed analysis of these developments.

David Wotherspoon, a partner with Fasken Martineau in Vancouver, has provided advice and expertise in more than 100 defamation matters. As a former news photographer, his curiosity about media issues transferred into his legal career as he pursued matters of defamation, publication bans, and other media issues. Many of David's cases involve protecting businesses that are targeted and need intense and swift action to safeguard their rights. He does not Twitter.

Christian Leblanc, a partner with Fasken Martineau in Montreal, specializes in media and communication law. He acts for some of Canada's larger media enterprises on issues relating to freedom of the press and freedom of speech. Currently he is acting for the CBC, La Presse newspaper, Astral Media Radio, Groupe TVA, Transcontinental Media and the Quebec Federation of Journalists in their bid to gain intervener status before the Supreme Court of Canada in a publication ban case.

© 2009 by David Wotherspoon and Christian Leblanc.]

¹ [1999] B.C.J. No. 622.

² [2005] B.C.J. No. 1993.

³ [1999] 4 All ER 609.

INVITATION TO OUR READERS

Do you have an article that you think would be appropriate for *Internet and E-Commerce Law in Canada* and that you would like to submit?

AND/OR

Do you have any suggestions for topics you would like to see featured in future issues of *Internet and E-Commerce Law in Canada*?

If so, please feel free to contact Michael A. Geist

@mgeist@uottawa.ca

OR

ieclc@lexisnexis.ca