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 12, NUMBER 2 Cited as (2011-12) 11 I.E.C.L.C. JUNE 2011

• TECH EMPLOYEE FIRED FOR EGREGIOUS COMPUTER USE — TERMINATION JUSTIFIED •

Maria Giagilitsis
Fasken Martineau DuMoulin LLP

Along with the extraordinary benefits accompanying today's rapidly advancing technology, comes an increasing vulnerability for employers who strive to hire the "best of the best" information technology groups. On the one hand, "wizard-like" computer skills are an invaluable asset — they can lead a company's growth while sharpening its competitive edge. On the other hand, these advanced skills can also be a source of weakness as management struggles to predict the numerous and complex ways in which a technology employee might abuse his or her position and even cause harm to the business. On December 3, 2010, Ontario arbitrators released a decision in *Sheridan College Institute of Technology and Advanced Learning v. Ontario Public Service Employee Union*, [2010] O.L.A.A. No. 632, in which they agreed with the termination of an employee for unauthorized computer use as well as an insolent Facebook posting.

Mere Technical Wrongdoings?

The grievor, Steve Rowe, was the consummate techy — at 36 years old, he was considered a technical wizard at the College, having been employed as an Infrastructure Analyst for 13 years. He occupied one of the highest paid bargaining unit positions at the College and, until the date that his employment was terminated, he had a clean disciplinary record and was provided with access to the College's most secure servers.

• In This Issue •

TECH EMPLOYEE FIRED FOR EGREGIOUS COMPUTER USE — TERMINATION JUSTIFIED
Maria Giagilitsis.....9

RETRACTING LIBEL LOST IN CYBERSPACE: IMPLICATIONS FOR THE NEW DEFENCE OF RESPONSIBLE COMMUNICATION
Matthew Nied.....12

PROPOSED REGULATIONS EFFECT THE ON-LINE INSURANCE ACTIVITIES OF DEPOSIT-TAKING FINANCIAL INSTITUTIONS
Stephanie Robinson and Ratika Gandhi.....14

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

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

Subscription rates: $200 per year (print or PDF)
$295 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.

What happened? Like many employees, Mr. Rowe blurred the boundary between his personal life and his professional life. More specifically, the grievor adopted a surplus College computer as his own, even naming it "Numb". Numb was hooked up to one of the College's most powerful network servers, which facilitated over $20 million in online transactions each year. Using the powerful system, the grievor was able to download thousands of copyrighted materials, including TV shows, movies, music, and games, all of which he stored on Numb. The grievor also downloaded pornographic videos and engaged in online chats with his girlfriend about their various sexual encounters, some of which purportedly took place on College premises.

In an ever bolder move, the grievor installed his own programming, which granted access to numerous colleagues and employees of the College as well as several family members and friends, none of whom were granted security clearance by the College to access the server. Essentially, the grievor was a bootleg entertainment dealer for a wide circle of colleagues, family and friends.

When a third party audit revealed some of the grievor's behaviour, the College conducted an investigation. The results of the investigation confirmed that the grievor had been engaging in the unauthorized activities for the better part of this decade. Not surprisingly, the grievor's employment was terminated.

That same day, the grievor posted a picture of the rear of a mountain climber on his Facebook page, adding an arrow pointing to the climber's buttocks with a caption inviting his manager to "kiss this". The grievor later apologized for the Facebook posting but only after being advised to do so by the union.

Grievance

The union grieved the termination of the grievor's employment, claiming that the College overreacted. According to the union, the discipline was too harsh given Mr. Rowe's previously clean discipline record and his apology for the Facebook posting. The union also relied heavily on the fact that the College had previous knowledge of the grievor's personal use of College computers for the purposes of downloading and storing music and other personal media.

Termination Justified

The arbitrators agreed that an employer's previous knowledge of an employee's wrongdoings may sometimes impact the appropriate level of discipline. In this case, however, the arbitrators found that the termination was justified for a number of reasons:

(a) Though the College had some knowledge of the grievor's personal computer use, the College had no idea of the extent to which the grievor abused his privileges.

(b) The College did not have any knowledge that the grievor programmed the computer to grant remote access to other employees of the College as well as the grievor's family and friends. Those other employees were also disciplined for their unauthorized access to the College server, thus demonstrating the severity with which the College perceived the grievor's conduct.

(c) The grievor was provided with an opportunity to explain his conduct during the investigation process. Rather than being candid about his activities, the grievor attempted to surreptitiously delete the personal contents from Numb just before the investigation meeting and was evasive during the investigation meeting itself.

(d) The grievor was employed in a position of trust, having access to highly sensitive information and enjoying a high level of security clearance. The arbitrators said that a person employed in this capacity is expected to exercise better judgement.

(e) The grievor's Facebook posting illustrated poor judgement and a total lack of remorse for his egregious conduct.

(f) The employer's evidence showed that the grievor had signed the College handbook, which specifically set out the College's rules and expectations about personal computer use.

Conclusion

Information technology employees often enjoy access to highly sensitive employer data and it seems that courts and arbitrators are becoming increasingly sensitive to the threats these skills can pose to an employers' business interests. The decision in *Sheridan College* demonstrates that an employee's lack of remorse, coupled with his or her disregard for the employer's business and financial interests, can justify firing even a highly paid employee with a long and clean service record. Although this decision arises in Ontario, it may well have application across the country.

[*Editor's note*: This article was re-published with the permission of the law firm Fasken Martineau DuMoulin, LLP, as well as the publishers of Northern Exposure, a blog written by the law firm's lawyers. Northern Exposure is produced in con-junction with HRHero.com. You can read more Northern Exposure blog posts at http://blogs.hrhero.com/northernexposure.

Maria Giagilitsis is a senior associate at Fasken Martineau DuMoulin LLP with a specialized practice, focusing on all aspects of human rights,

labour and employment law. Maria works closely with corporations, human resource professionals and in-house legal counsel, providing both emergent and long-term strategic advice in connection with a broad range of complex matters including the duty to accommodate, wrongful dismissal, and the negotiation, drafting and interpretation of collective agreements, employment agreements and severance agreements. Maria regularly leads educational training sessions for all levels of management, employees and human resource professionals on virtually all aspects of human rights and employment law and has also taught Employment and Human Rights law at George Brown College.]

• RETRACTING LIBEL LOST IN CYBERSPACE: IMPLICATIONS FOR THE NEW DEFENCE OF RESPONSIBLE COMMUNICATION •

Matthew Nied
Student-at-Law

Introduction

The Times, a national newspaper, published an article alleging impropriety on the part of a government official. In accordance with common practice, the newspaper also published the article on its website. When it learned months later of developments that had emerged since the date of publication, serious doubt arose about the truth of the allegations in the article. Although the newsprint version of the article had long since migrated to waste bins, the online version remained easily accessible on the internet. Understandably, the official asked the newspaper to remove the article from the internet, or update it to alert readers that its allegations might be false. The newspaper refused, and the defamatory words remained visible for the world to see.

This account illustrates that although the internet provides publishers with tremendous power to harm reputation, it also offers them an unparalleled power to mitigate reputational harm. Unlike traditional mediums of communication that preserve defamatory words in their original form, the web often permits internet publishers — such as online newspapers, bloggers, and "twitterers" — to immediately retract, edit, or remove publications that may be defamatory. An internet publisher's failure to make such efforts may have liability implications. Specifically, recent cases indicate that internet publishers may disqualify themselves from the application of the new defence of responsible communication by failing to retract, edit, or remove publications after becoming aware of developments which indicate that they may be defamatory. This article discusses these cases and considers the implications for internet publishers.

Defence of Responsible Communication

Once a plaintiff proves that an internet publication is defamatory, the publisher will be liable unless they establish a defence. In the recent case of *Grant v. Torstar*,[1] the Supreme Court of Canada created the new defence of responsible communication. The defence is available to anyone who publishes in any medium.[2] To gain the protection of the defence, the defendant must establish two elements: that the publication concerned a matter of public interest, and that the publication was responsible.[3]

Recent English cases suggest that an internet publication may not be responsible if the publisher failed to retract, edit, or remove it after

becoming aware of subsequent developments which indicate that it might be defamatory. Although these authorities concern the English defence of responsible journalism, that defence provided the model for the defence of responsible communication. Accordingly, these authorities may be influential in future cases.[4]

In *Flood v. Times Newspapers Ltd.,*[5] a newspaper published an article in print and on its website alleging that the plaintiff, a police officer, was under investigation for taking bribes. The plaintiff was cleared of corruption charges more than a year later. Although the plaintiff notified the newspaper of these developments, the original article was left unaltered on its website. The trial court held that the internet publication was originally protected by the defence of responsible journalism, but not in respect of the period for which the publication remained available on the internet after the publisher gained knowledge of the developments. This conclusion was upheld by the English Court of Appeal, which noted that, in these circumstances, "any responsible journalist would appreciate that those allegations required speedy withdrawal or modification".[6]

The same conclusion was reached in the earlier case of *Loutchansky v. Times Newspapers Ltd*.[7] There, a newspaper published articles in print and on its website accusing the plaintiff of involvement in criminal activities. When the plaintiff commenced a defamation action with respect to the printed articles, the newspaper neglected to attach a qualification to the articles on its website to alert readers that legal proceedings had been brought in relation to their truth. Although the trial court found that the defence of responsible communication applied to the print publications, it did not apply to the internet publications because they had not been updated or qualified to reflect the developments. The decision was upheld by the English Court of Appeal, which concluded that the "failure to attach any qualifications to the articles published ... on [the] website could not possibly be described as responsible journalism."[8]

Implications

Our courts may apply the reasoning in *Flood* and *Loutchansky* to deny internet publishers the protection of the defence of responsible communication in similar circumstances. To minimize their risk of liability, internet publishers should take immediate steps to retract, update, or remove their publications once they receive notice of developments which indicate that they may be defamatory.

These authorities need not be read to suggest that internet publishers must bear the burden of continually monitoring their publications for developments, however. In *Flood* and *Loutchansky*, the courts found that the internet publishers had received ample notice that their publications might be defamatory. In *Loutchansky,* the defendant was aware that the internet publication was potentially defamatory because legal proceedings had been brought in respect of the print version, which was identical. Likewise, in *Flood,* the plaintiff notified the defendant of the findings of an investigation that demonstrated that the allegation in the article was false. The publishers in both of these cases were found to have acted irresponsibly because they failed to react after receiving notice of these developments.

These circumstances may be distinguishable from cases in which internet publishers fail to receive notice of developments through no irresponsibility of their own. If such a distinction were not made, internet publishers might effectively be forced to monitor their voluminous archives of publications for developments. This

might restrict their ability to maintain publicly accessible internet archives, and thereby violate their *Charter* right to freedom of expression.

Internet publishers may also reduce their risk of liability by ensuring that their internet publications clearly display the original date of publication, particularly where those publications involve subject matter likely to give rise to new developments. In addition, internet publishers may consider placing a notice on their publications to alert readers that their contents reflect the facts known to the publisher on the original date of publication. Although there is no judicial guidance on this point, this practice might support an internet publisher's argument that its publication was responsible for the purposes of the defence.

Finally, it may be preferable for internet publishers to update or retract their publications in response to developments instead of editing or removing them. After an article is published on the internet, its defamatory content may be reproduced beyond the control of the publisher and remain easily accessible through search engines. As a result, defamatory remnants may linger on the internet long after the removal of the original publication. Adding a prominently-placed retraction or update to the original publication may be seen to increase the likelihood that readers will be alerted to the potential falsity of any related libel, which may support a finding of responsibility on the part of the publisher. This practice also has the benefit of minimizing interference with the publisher's freedom of expression and protecting the public's interest in the availability of historical records.[9]

[*Editor's note*: Matthew Nied, B.Comm. (Alberta), LL.B. (Victoria) is currently clerking at the Supreme Court of British Columbia. He will commence articles in Vancouver in September 2011. The views expressed are personal opinions and not those of the judiciary.]

---

1 [2009] S.C.J. No. 61, 2009 SCC 61.

2 *Ibid.* at para. 96.

3 *Ibid.* at para. 98.

4 The reasoning in these authorities depends on the application of the English multiple publication rule. This rule holds that a defamatory statement is published afresh every time it is accessed on the internet. As a consequence, an internet publication that may have been originally responsible for the purposes of the defence may cease to be responsible when it is accessed by a reader after new developments have emerged. The rule has been adopted in Canada: see *e.g. Carter v. B.C. Federation of Foster Parents Assn.*, [2005] B.C.J. No. 1720, 2005 BCCA 398 at para. 20.

5 [2009] EWHC 2375 (QB).

6 [2010] EWCA Civ 804 at para. 78.

7 [2001] EWCA Civ 1805.

8 *Ibid.* at para. 79. When leave for a further appeal was refused, the newspaper brought a complaint to the European Court of Human Rights. The Court held that requiring the publisher to update their publication in the circumstances did not constitute a disproportionate interference with freedom of expression: *Times Newspapers Ltd (Nos. 1 and 2) v. United Kingdom,* [2009] EMLR 14 at para. 47.

9 Removal of the original publication may be preferable in circumstances where there is no public interest in allowing the publication to remain accessible, there has been limited reproduction, or an update would increase reputational harm by inviting further attention to the matter.

• PROPOSED REGULATIONS AFFECT THE ON-LINE INSURANCE ACTIVITIES OF DEPOSIT-TAKING FINANCIAL INSTITUTIONS •

Stephanie Robinson and Ratika Gandhi
McMillan LLP

After much anticipation, the federal government released the proposed regulations to amend the Insurance Business (Banks and Bank Holding Companies) Regulations and the Insurance Business (Authorized Foreign Banks) Regulations by publication in the Canada Gazette on February

12, 2011. The proposed amendments are intended to provide greater clarity and consistency about the types of authorized insurance products that are available through the branches and online web pages of deposit-taking financial institutions. The amended regulations propose:

1. to generally extend to the web pages of deposit-taking financial institutions the application of the regulatory framework that currently applies to the insurance business activities in branches;
2. to ensure that the promotion of insurance products by deposit-taking financial institutions is related to the core business of these institutions (such as credit, mortgage or travel-related insurance);
3. to prevent deposit-taking financial institutions from using their web pages to promote non-authorized insurance products (such as life, health, home and auto insurance), which is not permitted in their branches; and
4. to prohibit the promotion of, or web links to, insurance other than authorized insurance from all web pages of deposit-taking financial institutions.

The regulations were made necessary by the evolving use of technology by deposit-taking financial institutions and consumers. In addition, several technical amendments are proposed, including corrections to the French versions of the Insurance Business Regulations to ensure consistency with the English versions.

Background

The federal Bank Act, S.C. 1991, c. 46, prohibits deposit-taking financial institutions from engaging in the business of insurance except as permitted by regulation. Under the regulations, permitted and prohibited insurance business activities vary according to whether they take place inside or outside a bank branch, or whether they relate to an "authorized type of insurance". Generally, the regulations provide that deposit-taking financial institutions may only promote an insurance company, agent or broker (an "Insurance Entity"), or an insurance policy of an Insurance Entity, if either (i) the promotion takes place outside of a bank branch and is directed to a large class of people (such as all holders of credit cards issued by the deposit-taking financial institution), or (ii) the Insurance Entity deals only in an "authorized type of insurance". The regulations identify the following as "authorized type of insurance":

- Insurance covering losses related to credit or charge cards that is provided as a feature of such cards without request and without an individual risk assessment;
- Extended warranties on purchases charged to such cards;
- Coverage of liabilities arising from car rental contracts secured with such cards;
- Creditors' life, disability or loss of employment insurance;
- Creditors' vehicle inventory insurance;
- Export credit insurance;
- Mortgage insurance; or
- Travel insurance.

The current rules prohibit the sale or marketing of policies of life, health, home and auto insurance in branches. There are also a variety of restrictions on the ability of a deposit-taking financial institution to share information about its

customers or employees with an Insurance Entity. However, the current regulations do not address on-line promotion of insurance products or whether a bank web page qualifies as a "branch". In 2009, the Office of the Superintendent of Financial Institutions ("OSFI") was asked to rule on the question of whether, for the purpose of the Insurance Business (Banks and Bank Holding Companies) Regulations, a bank website is a bank branch. OSFI concluded in Ruling No. 2009-02 that for the purposes of the regulations, a bank website is not a branch. OSFI Rulings describe how OSFI has applied or interpreted certain provisions of the Bank Act, and the regulations or guidelines thereunder, but are not necessarily binding on OSFI's consideration of subsequent transactions. In response to the OSFI Ruling, the Minister of Finance announced that the federal government planned to tighten regulations regarding the promotion of non-authorized insurance on the web pages of deposit-taking financial institutions. The federal government felt the need to provide clarity on this issue in the regulations in light of the growing use of web pages by deposit-taking financial institutions.

Proposed Changes

The proposed regulations will extend current government policy about the permitted and prohibited insurance promotion activities of deposit-taking financial institutions to the web pages of such institutions, and will help ensure consistency between the promotion of insurance products permitted on the web pages of deposit-taking financial institutions and the promotion that is permitted in their branches. The stated objective of the regulations is to limit the types of insurance that deposit-taking financial institutions are permitted to sell or promote to the "authorized types of insurance" that are ancillary to the main business of such institutions. The regime will prohibit the promotion of, and web links to, non-authorized insurance from a "bank web page". Section 2 of the existing regulations will be amended to include a definition of "bank web page":

> *a web page that a bank uses to carry on business in Canada, including any information provided by the bank that is accessible on a telecommunications device. It does not include a web page that is only accessible by employees or agents of the bank.*

More specifically, the proposed regulations will prohibit a deposit-taking financial institution from providing access on a bank web page to a web page (either directly or indirectly through another web page) on which there is promotion of an Insurance Entity, or an insurance policy of an Insurance Entity, that does not deal exclusively in authorized types of insurance.

[*Editor's note*:
This article was originally edited by, and first published on www.internationallawoffice.com — the Official Online Media Partner to the International Bar Association, an International Online Media Partner to the Association of Corporate Counsel and European Online Media Partner to the European Company Lawyers Association.

Stephanie Robinson is a partner in the firm's Financial Services Group. Stephanie's practice focuses on corporate finance and structured finance transactions, including domestic and cross-border commercial debt financing, syndicated lending, asset-based lending, and securitizations.

Ratika Gandhi is currently an articling student at McMillan LLP, and previously summered with the firm in the Business Law Group. Ratika is a recent graduate of Osgoode Hall Law School. Prior to law school, Ratika obtained an Honours Bachelor of Arts and Science degree from McMaster University.]