CANADIAN PRIVACY LAW REVIEW

Volume 10 • Number 2 January 2013

In This Issue:

How Far Should Privacy Commissioners Roam?—Part 1

Christopher Berzins
Senior Legal Counsel
Ontario Securities Commission

I. Introduction

In July 2008, highly regarded privacy expert and then-editor of *PrivacyScan*, Murray Long, commented favourably on the efforts of Information and Privacy Commissioner of Ontario Ann Cavoukian to bring the power of "moral suasion" to bear on a matter clearly outside her jurisdiction, that being a litigious dispute in the United States involving Google and Viacom. Commissioner Cavoukian had written an open letter to Sergey Brin and Peter Fleischer, urging Google to appeal a court ruling that required Google to disclose information about YouTube users to Viacom.[1] I've always deeply respected Mr. Long's views, and I do appreciate the point he was making here.[2] However, in my view, the Google/Viacom example also raises concerns about the potential problems that can arise when privacy commissioners stray too far afield.

When privacy commissioners exercise specific investigatory or adjudicatory powers (assuming they have them[3]), concerns about possible excesses of jurisdiction can be addressed via judicial review. However, when they rely on their "softer" powers, such as public comment, criticism, and moral suasion to advance a position, or when they expend resources on issues that arguably fall outside their mandate, there is little to hold them in check because such activities will be difficult to review in the courts.[4] This is troubling because excesses of jurisdiction with respect to these matters do have significant implications for oversight and enforcement of privacy legislation.

Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

ISBN 0-433-44417-7 ISSN 1708-5446
ISBN 0-433-44418-5 (print & PDF)
ISBN 0-433-44650-1 (PDF)
ISSN 1708-5454 (PDF)

Subscription rates: $255.00 (print or PDF)
$395.00 (print & PDF)

It must be remembered that privacy commissioners are creatures of statute and their jurisdiction to publicly comment, criticise, and advocate flows from the statutes that they are assigned responsibility for overseeing and enforcing. Even though privacy issues extend well beyond provincial and national boundaries and as much as this may invite co-operation and collaboration amongst oversight bodies, there are still limits that must be respected. Privacy Commissioner of Canada Jennifer Stoddart clearly recognised as much in a 2012 speech where she noted that: "As Commissioners, we must proceed in our work *cognizant and respectful of each other's jurisdiction* [emphasis added]."[5]

This article considers some of the concerns that may arise when privacy commissioners become involved in issues that may be outside their jurisdiction and expend resources on these matters. There are four issues that I examine. The first is whether privacy commissioners enjoy an essentially unfettered jurisdiction to comment broadly on privacy issues affecting all individuals residing within their territorial jurisdiction. The second concerns making public comments about matters that have clearly been assigned to other privacy commissioners. The third is public involvement in privacy-related issues that fall within the bailiwick of other bodies, such as arbitrators, courts, or other adjudicators. Finally, there is the expenditure of resources on matters that appear to be entirely, or for the most part, outside a privacy commissioner's jurisdiction. Many of the discussed examples, which I'm most familiar with, involve Ontario's Information and Privacy Commissioner. But these issues can arise in any jurisdiction, in large part, because privacy concerns frequently transcend geographic boundaries.

To be clear, I think it is entirely proper for privacy commissioners to comment publicly on their concerns about the scope and limits of their jurisdiction and to bring this to the legislature's attention.[6] It is also appropriate for privacy commissioners to take a broad reading of the powers assigned to them.[7] However, it is another matter entirely to comment unilaterally in a substantive manner or expend resources with respect to matters clearly falling outside one's jurisdiction. I also fully appreciate that cooperation and

collaboration with a range of entities should be encouraged to advance effective privacy protection.[8] But a healthy respect for jurisdictional boundaries is also important if privacy commissioners are to retain their influence and credibility, avoid the risk of hampering the efforts of their colleagues, and expend their resources prudently.

II. Who Does a Privacy Commissioner Speak for?

Former Privacy Commissioner of Canada George Radwanski regularly described himself as the "independent guardian and champion of the privacy rights of Canadians."[9]

Commissioner Cavoukian has also spoken out on federal initiatives on a number of occasions because, in her view, "my mandate includes commenting on *developments that affect the personal privacy of Ontarians* [emphasis added]."[10] In addition, her news releases state that: "A vital component of the Commissioner's mandate is to help *educate the public about access and privacy issues* [emphasis added]."[11]

On a cursory reading, these comments might appear unremarkable, involving at most a somewhat generous view of the mandate of the respective offices. However, in my view, the way both commissioners characterised their jurisdiction over privacy matters raises important concerns. Aside from former Commissioner Radwanski's implicit slight to provincial privacy commissioners,[12] his description of his role was a considerable overreach. Commissioner Radwanski was only responsible for overseeing the federal government and the federally regulated private sector; he was not responsible for the privacy rights of Canadians with respect to their dealings with their provincial and municipal governments nor, at that time, with the provincially regulated private sector.[13] His jurisdiction to publicly comment, conduct research, and educate the public was also limited; the *Privacy Act*[14] is largely silent in this regard,[15] and the *Personal Information Protection and Electronic Documents Act* [*PIPEDA*],[16] which does contain extensive powers to conduct research and promote the purposes underpinning the legislation,[17] was still confined in application at that point to the federally regulated private sector.

Similarly, Commissioner Cavoukian's view of her mandate seems to extend well beyond what is set out in the statutes that establish her jurisdiction. The *Freedom of Information and Protection of Privacy Act* [*FOIPPA*],[18] the *Municipal Freedom of Information and Protection of Privacy Act* [*MFOIPPA*],[19] and the *Personal Health Information Protection Act, 2004* [*PHIPA*][20] all provide the commissioner with an explicit mandate to publicly comment on the "privacy protection implications of proposed legislative schemes or government programs"[21] and to engage in privacy-related research. However, these grants of authority are framed explicitly in terms of each of the statutes in question.[22] Commissioner Cavoukian has positioned some of her comments on certain federally initiated law enforcement matters as linked to her responsibility for addressing law enforcement issues arising under the *FOIPPA* and *MFOIPPA*.[23] But, in my view, that crosses the dividing line between the responsibility for assessing whether provincial and municipal police are complying with their privacy obligations under the *FOIPPA* and *MFOIPPA* when applying federal legislation and commenting on the merits of federal legislation at first instance.

With respect to the scope for public comment and research on privacy-related matters, the most significant jurisdictional constraint on Ontario's commissioner is the IPC's lack of a private sector privacy oversight mandate. Many emerging privacy concerns are now being generated by private sector entities such as internet search firms, social networking sites, and commercial data profilers.[24] But without private sector oversight responsibilities, Ontario's commissioner would seemingly be limited in her ability to comment on private sector pri-

vacy issues or to engage private sector entities such as Google, Facebook, or IBM, unlike other Canadian privacy commissioners who have private sector privacy oversight responsibilities. However, that has not played out in practice.[25]

What, one might ask, is the harm in privacy commissioners taking an expansive view of their jurisdiction and their privacy constituency? And shouldn't we be supportive of *any* research, education, or public commentary that help raise the profile of privacy concerns and the public's understanding of such issues? Quite simply, there are serious risks attached to this; it is a very slippery slope. This can take privacy commissioners into territory that others have primary responsibility for. This is risky because it may interfere with others' ability to respond to the aforementioned issues. It may also impair the credibility of all concerned if these incursions reveal differing views about how an issue ought to be addressed.[26] And it may also lead to the questionable expenditure of scarce resources on matters that are not part of the privacy commissioner's mandate.

Similar issues can arise when there are serious gaps in legislative coverage, as is clearly the case with workplace privacy issues in Ontario.[27] While there may be an understandable temptation to fill such gaps, this can again take privacy commissioners into territory not assigned to them by the legislature. As suggested earlier, it is entirely appropriate for privacy commissioners to bring such jurisdictional concerns to the legislature's attention. But it is another matter to expend resources addressing issues outside their jurisdiction in a substantive manner.

In my view, privacy commissioners do not enjoy an unrestricted mandate to address all privacy-related matters affecting individuals who reside within their territorial jurisdiction. Some of these matters have been assigned to their colleagues or to other adjudicative bodies, and these lines of authority need to be respected. What follows are some examples of why this is the case.

III. Entering Other Commissioners' Territory

In July 2011, a passenger on a bus in Gatineau, Quebec, filmed the driver completing paper work while driving. The video was then posted on YouTube where it generated considerable attention.[28] The president of the Amalgamated Transit Union ("ATU"), which represented the driver in question, asked the Société de Transport de l'Outaouais ("STO") to prohibit passengers from being able to video record drivers, suggesting, apparently, that this was a violation of the driver's privacy.[29]

Shortly after that, Commissioner Cavoukian commented on the issue. In an interview with CBC News, Commissioner Cavoukian acknowledged that the issue fell outside her jurisdiction but went on to say "[i]t is outrageous to characterize this as a privacy invasion because it is not a privacy issue." She added that "[w]hen you are performing a job, in this case a public service involving public safety … you do not have a privacy interest because your work should be transparent."[30]

This story received far less attention than should have been the case because, in my view, Commissioner Cavoukian's comments raised some troubling issues. The most obvious is the risk of pronouncing in such a categorical manner when all of the facts may not have been on the table, especially the manner in which the union may have presented the issue in its discussions with the STO. Second, and closely related, is the remarkably dismissive nature of the commissioner's comments. I find it surprising that the union's position could be discounted in such a sweeping manner. After all, some highly respected privacy scholars such as Helen Nissenbaum have argued persuasively that there are legitimate privacy claims that can be advanced in public settings.[31] It is hardly a stretch to

suggest that this might extend to the employment context with respect to jobs that are performed to a large extent in a public venue.[32]

But the bigger concern, as I see it, is the impact of such comments if the matter had been raised before Quebec's Commission d'accès à l'information. If, for example, the ATU complained that the STO was not adequately addressing the privacy interests of its membership by refusing to prohibit the recording of drivers,[33] it would not be surprising if it had reservations about how Commissioner Cavoukian's comments might affect the outcome. Those comments could also put the Commission d'accès à l'information in a difficult position in the event that it saw some merit to the union's position. It would then have to publicly distance itself from the public pronouncements of another Canadian privacy commissioner. Investigators and adjudicators are usually restrained in publicly commenting on matters they are considering or that may come before them. In my view, the same sort of prudence ought to have been exercised in this instance, the appropriate response being that this was a matter for the Commission d'accès à l'information to address.

Ontario's commissioner has also involved herself frequently in matters falling within the jurisdiction of the Privacy Commissioner of Canada under both the *Privacy Act* and *PIPEDA*. With respect to the *Privacy Act*, Commissioner Cavoukian has commented regularly on the federal government's "lawful access" initiatives, going as far as sending a detailed legal analysis of the legislation to Minister of Public Safety Vic Toews and to Minister of Justice and Attorney General of Canada Rob Nicholson.[34] While she has acknowledged that federal legislation does not fall within her jurisdiction, in her defence she has said that "[t]his is such an important issue, it can't be limited by boundaries."[35] She also commented recently on the federal government's plan to install listening devices in government airports and border crossings. After again acknowledging that was an issue falling within federal jurisdiction, she characterised the federal proposal as "appalling."[36] And in 2009, her office released a paper that discussed how the concept of *Privacy by Design* could be employed to reduce the intrusiveness of passenger scanning in airports,[37] another matter clearly falling within the jurisdiction of the Privacy Commissioner of Canada.

If anything, Commissioner Cavoukian has been even more involved in private sector privacy matters with little acknowledgement that most of these issues are largely the responsibility of the Privacy Commissioner of Canada[38] or other provincial commissioners who have private sector privacy oversight responsibilities.[39] A prime example would be Commissioner Cavoukian's collaborative engagement with Facebook in developing a brochure aimed at informing students of the privacy implications of posting personal information to social networking sites.[40] Commissioner Cavoukian has explained that she was approached by Facebook executives in 2006 "seeking [her] input on their privacy measures."[41]

Aside from the obvious fact that this is simply not within her jurisdiction, whether approached by Facebook or not, this type of involvement raises a number of concerns. First, Facebook's privacy practices have been the subject of several significant complaint investigations by the Privacy Commissioner of Canada.[42] These types of collaborative efforts with private sector bodies run the risk of undercutting the leverage and credibility of the responsible commissioner who may be required to conduct such investigations.

Second, developing private sector privacy guidance in concert with private sector entities (or on one's own initiative) creates a risk that a privacy commissioner may take a position or frame an issue in a manner that the responsible commissioner may not be fully comfortable with, thereby impeding the latter's ability to deal with it in a manner he or she deems appropriate. This point is underscored by the

fact that a number of those privacy commissioners who share private sector privacy oversight responsibilities have issued joint guidance to private sector organizations to promote "consistency in the expectations of Commissioners."[43] And recently, these same commissioners arrived at a memorandum of understanding designed to facilitate "cooperation and collaboration in policy, enforcement, public education, and compliance."[44]

Third, collaborative efforts with the private sector may encourage private sector entities to engage in a type of forum shopping that again runs the risk of undercutting the responsible privacy commissioner.[45]

The IPC's social networking guidance developed in concert with Facebook is not its only collaborative effort with the private sector. Other private sector entities the IPC has partnered with on private sector privacy issues include IBM, Intel, Hewlett-Packard, Microsoft, the Ponemon Institute, and the Canadian Marketing Association. And Commissioner Cavoukian's office has spoken frequently to private sector audiences about their privacy obligations, even though the IPC has no responsibility (aside from *PHIPA*) for these matters. Since 2002, her office has made well over 30 such presentations, frequently, on the theme of privacy as a competitive business advantage.[46]

Leaving aside for now the issue of expenditure of limited resources, any potential benefits of unilateral involvement in matters assigned to other privacy commissioners are clearly offset by the risks entailed. Such involvement may interfere with the responsible commissioners' approaches to oversight and enforcement, places commissioners in the unenviable position of having to distance themselves from another privacy commissioner in the event there is a difference in views, and, potentially, undercuts commissioners' credibility. For these reasons, such involvement should clearly be avoided.

[*Editor's note*: The views expressed here are entirely of the author and are not intended to represent those of the Ontario Securities Commission.]

---

1 Commissioner Cavoukian, "Google Viacom Order and the Force of Moral Suasion," *PrivacyScan* (July 15, 2008).

2 In Mr. Long's view, Commissioner Cavoukian's open letter "got to the point quicker and brought some underlying privacy concerns into more prominence" than might have been the case had a complaint been made to a commissioner with the power to investigate. I certainly don't disagree with that assessment, but it still leaves open any number of questions about the appropriate scope for comment on such issues.

3 There are issues that arise when privacy commissioners make recommendations rather than issue orders or where their investigatory powers are lacking. For example, in *Reynolds v. Binstock*, [2006] O.J. No. 4356 (Ont. Sup. Ct.), the Divisional Court held that the privacy investigations of Ontario's Information and Privacy Commissioner were not subject to judicial review because she was not exercising an adjudicative power.

4 Administrative agencies' reliance on informal powers has been a longstanding concern in the United States in large part because these activities are "shielded from judicial review." See James O. Freedman, "Summary Action by Administrative Agencies," U. Chicago L. Rev. 40, no. 1 (1972): 38; Ernest Gellhorn, "Adverse Publicity by Administrative Agencies," Harv. L. Rev. 86 (1973): 1380; and, most recently, Nathan Cortez, "Adverse Publicity by Administrative Agencies in the Internet Era," B.Y.U.L. Rev. (2011): 1372. And, as the Divisional Court's decision in *Reynolds v. Binstock* makes clear, even investigatory activities may not be subject to judicial oversight. *Supra* note 2.

5 See *Privacy Protection in Canada—Keeping Pace with Advancing Global Norms*, Remarks at the 2012 Access and Privacy Conference, organised by the University of Alberta, June 14, 2012, Edmonton, Alberta.

6 An excellent example of bringing jurisdictional limitations to the attention of the legislature is the work of Ontario Ombudsman André Marin who has repeatedly pushed for an expansion of his mandate to allow him to investigate municipalities, universities, school boards, hospitals, children's aid societies, long-term care homes, and the police. In 2007, he stated, "I also strongly believe that we must speak out against shortcomings in our mandate." See "Innovate or Perish," Can. J. Admin. L. & Prac. 20 (2007): 101. Mr. Marin continues to raise this issue, most recently, at some length in his Annual Report for 2011–12. He is also seeking an expansion of his jurisdiction to allow him to investigate when public services are privatised, citing the example of Ornge.

In comparison to Mr. Marin's efforts, the IPC has not raised jurisdictional concerns with anything near the same vigour and has said relatively little about the legislative changes in 1995 that effectively ousted the privacy rules for government employees or about the statutory deficiencies that undercut the IPC's ability to investigate privacy complaints effectively.

7 In the past, I have been highly critical of the Office of the Privacy Commissioner of Canada for its insistence on taking an extremely narrow reading of its powers to publicly identify complaint respondents under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*]. See "Three Years under the *PIPEDA*:

A Disappointing Beginning," C.J.L.T. (2004): 113; "Reviewing *PIPEDA*: A Chance to Change Direction," Can. Priv. Law Rev. 3, no. 10 (2006): 109; and "Picking Cherries or Squeezing Lemons?: Some Further Thoughts on the Ombudsman Model of Privacy Oversight," Can. Priv. Law Rev. 8, no. 1 (2010): 1.

Ontario Ombudsman André Marin is also a strong advocate of taking an expansive view of one's jurisdiction. In his view, "I have always maintained that the Ombudsman's mandate should be given a broad, generous and liberal interpretation." See "Innovate or Perish," *supra* note 7.

8 I strongly encouraged the use of such collaborative approaches in a 2004 paper criticising the manner in which the Privacy Commissioner of Canada had conducted oversight and enforcement of *PIPEDA.* See "Three Years under the *PIPEDA*: A Disappointing Beginning," *supra* note 8.

9 See *Address by the Privacy Commissioner of Canada to the Privacy Lecture Series* (March 26, 2001, Toronto).

10 Letter to Minister of Public Safety Vic Toews and Minister of Justice and Attorney General of Canada Robert Nicholson (October 31, 2011).

11 The IPC's news releases regularly use this language in the *About the IPC* section.

12 This is consistent with what Murray Long characterised as Commissioner Radwanski's "imperial arrogance." Mr. Long reported: "I am aware of behind the scenes efforts he made to prevent provincial commissioners from attending the annual International Data Commissioners Conference, believing that only national, not regional commissioners, should be allowed to attend." *PrivacyScan* (September 26, 2008): 6.

13 Responsibility for the provincially regulated private sector only came into effect in 2004 in those provinces that had not passed legislation deemed to be substantially similar to *PIPEDA*.

14 R.S.C. 1985, c. P-21.

15 Section 60 of the *Privacy Act* allows the Commissioner to carry out privacy-related "studies" on the referral of the Minister of Justice.

16 *PIPEDA*, *supra* note 7.

17 *Ibid*., s. 24.

18 R.S.O. 1990, c. F.31.

19 R.S.O. 1990, c. M.56.

20 S.O. 2004, c. 3, Schedule A.

21 *FOIPPA*, *supra* note 18, s. 59(a).

22 In each case, the jurisdiction to conduct privacy-related research is framed in terms of "this Act."

23 In her letter to Ministers Toews and Nicholson on October 31, 2011, Commissioner Cavoukian noted that her mandate included "overseeing law enforcement compliance with privacy legislation in Ontario" and suggested that the government's "proposed surveillance regime will have a substantial impact on the privacy rights of Ontarians, law enforcement functions, and the role of my office."

24 With respect to commercial data profilers, see Chris Hoofnagle, "Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement," N.C.J. Int'l L. & Com. Reg. 29 (2004): 595; Joshua Simmons, "Buying You: The Government's Use of Fourth Parties to Launder Data about 'the People,'" Colum. Bus. L. Rev. (2009): 950; and Amitai Etzioni, "The Privacy Merchants: What Is to Be Done?," U. Pa. J. Const. L. 14, no. 4 (2012): 929.

25 In a 2004 news release, it was stated very clearly that: "The IPC regularly partners with private-sector organizations to advance privacy issues, practices, and technologies." See *Tools Now Available to Help Businesses Wrestling with Compliance under New Privacy Laws* (March 3, 2004).

26 An extreme illustration of such a conflict involved a critical open letter that former Commissioner Radwanski sent to Information Commissioner John Reid with respect to the issue of access to the prime minister's agendas under the *Access to Information Act*, R.S.C. 1985, c. A-1. This was clearly a matter squarely within the Commissioner Reid's jurisdiction, but Commissioner Radwanski chose to express his disagreement with Commissioner Reid in a very strong and public manner. See *Privacy Commissioner George Radwanski Writes to Information Commissioner John Reid Regarding Prime Minister's Agendas Case*, May 10, 2001, <http://www.priv.gc.ca/media/nr-c/02_05_b_010510_e.asp>.

27 For two reasons, workplace privacy issues fall outside the IPC's mandate. First, the provincial government's failure to introduce private sector privacy legislation resulted in *PIPEDA* applying to the provincially regulated private sector as of 2004. However, this did not extend to collection, use, and disclosure of personal information in an employment context, which remained a matter of provincial competence. Second, amendments to the *FOIPPA* and *MFOIPPA* that were introduced in 1995 excluded labour relations and employment-related information from the scope of the legislation, thereby ousting the privacy rules in this context. See *Labour Relations and Employment Statute Amendment Act, 1995*, S.O. 1995 c. 1, Schedule A, ss. 82–83.

28 According to one news account, the video received more than 130,000 hits in less than a month. See *Video of Bus Driver Violated Privacy, Union Says,* CBC News, August 10, 2011, <http://www.cbc.ca/news/canada/ottawa/story/2011/08/10/ott-gatineau-bus-driver-youtube-no-hands.html>.

29 *Ibid*. The quotes attributed to Felix Gendron, the president of the ATU, do not actually refer to a privacy violation, but the news accounts do say that the union had claimed that the filming constituted a violation of the "driver's privacy rights."

30 See *Ont. Privacy Commissioner Disputes Bus Union*, CBC News, August 11, 2011, <http://www.cbc.ca/news/technology/story/2011/08/11/ottawa-busdriver-privacy.html>.

31 In Nissenbaum's view: "The notion that when individuals venture out in public—a street, a square, a park, a market, a football game—no norms are in operation, that 'anything goes,' is pure fiction." See "Privacy as Contextual Integrity," Wash. L. Rev 79 (2004): 121. See, as well, "Protecting Privacy in an Information Age: The Problem of Privacy in Public," Law & Phil. 17 (1998): 559.

32 While one can think of cases in which video recording individuals in an employment context has been of significant public importance (*e.g.*, the beating of Rodney King by the LAPD, the RCMP's restraint of Robert Dziekanski), I think there are many other instances in which such recordings are highly questionable especially when these recordings are uploaded to the Internet.

33 Commissioner Cavoukian was equally dismissive about the union's request to ban recording of drivers. According to her, the union's proposal was "crazy." See *Commissioner Says Privacy Can't Be Used as Defence in STO Case*, August 11, 2011, <http://ottawa.ctvnews.ca/commissioner-says-privacy-can-t-be-used-as-defence-in-sto-case-1.682050>.

34 The 19-page legal analysis of the proposed federal legislation that was sent to Ministers Toews and Nicholson on October 31, 2011, is available on the Commissioner's web

site. <http://www.ipc.on.ca/english/About-Us/Whats-New/Whats-New-Summary/?id=230>.

35 See *Canada's Expanding Surveillance 'Should Scare You': Privacy Watchdog*, *National Post*, November 29, 2011, <http://news.nationalpost.com/2011/11/29/canadas-expanding-surveillance-should-scare-you-privacy-watchdog/>.

36 Richard Brennan, *Harper Government Backs down on Plans to Eavesdrop on Travellers' Conversations*, *Toronto Star*, June 19, 2012, <http://www.thestar.com/news/canada/politics/article/1213627--harper-government-backs-down-on-plans-to-eavesdrop-on-travellers-conversations>.

37 See *Whole Body Imaging in Airport Scanners: Building in Privacy by Design*, published March 2009, updated June 2009, <http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf>.

38 Although the Privacy Commissioner of Canada has jurisdiction under *PIPEDA* with respect to the commercial activities of private sector entities in Ontario, this does not extend to employment matters, which remain a matter of provincial responsibility.

39 When Ontario's commissioner engages private sector entities that have a global presence, such as Google or Facebook, this may have an impact on other provincial commissioners who have private sector oversight responsibilities and who may be dealing with these same entities under their private sector privacy statutes.

40 *When Online Gets out of Line*, published in October 2006, <http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf>.

41 *Social Networking and Privacy: You Must Architect Both into the Service You Provide*, presentation at the International Symposium: Privacy in the Age of Social Network Services, Strasbourg, France, October 13, 2008, <http://www.ipc.on.ca/english/Resources/News-Releases/News-Releases-Summary/?id=807>.

42 See *PIPEDA* Case Summary 2009-008 ("CIPPIC complaint"), *PIPEDA* Report of Findings 2011-005, *PIPEDA* Report of Findings 2011-006, and *PIPEDA* Report of Findings 2012-02, <http://www.priv.gc.ca/index_e.asp>.

43 For example, on April 17, 2012, the Federal, British Columbia, and Alberta privacy commissioners issued joint guidelines to private sector organizations with respect to their privacy obligations. See *Getting Accountability Right with a Privacy Management Program*, <https://www.privacyassociation.org/resource_center/getting_accountability_right_with_a_privacy_management_program>.

44 The Memorandum of Understanding between the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta, and the Office of the Information and Privacy Commissioner of British Columbia was with respect to "Cooperation and Collaboration in Private Sector Privacy Policy, Enforcement, and Public Education." It was signed in November 2011.

45 Whether initially intended or not, this may result in generating goodwill with one commissioner that can then be used as leverage with the responsible body, placing the latter in a difficult position.

46 These do not include presentations to private sector audiences involving personal health information, the smart grid, identity theft, or technologies such as RFID, biometrics, or cloud computing.

Social Media & Employees: When Every Little Thing Is Searchable

Timothy M. Banks
Partner
Fraser Milner Casgrain LLP

Battles in the United States, the United Kingdom, and Canada

The scope of an employer's right to discipline or terminate an employee for indiscreet or inappropriate remarks in social media is far from settled. It is not surprising that organizations are paying attention to the social media activities of employees. Social media can become an extension of the workplace when used by groups of employees to discuss workplace matters. However, unlike other forums and mediums, an indiscreet comment on social media has the potential to "go viral" (or at least be seen by hundreds, if not thousands of people). The activities of employees outside of work have the potential to negatively affect, even transiently, the reputation and goodwill of the organization.

Certainly there are cases of senior officers who may be reasonably considered to be fiduciaries and spokespersons of the organization being terminated or embarrassed by inappropriate use of social media. However, what is interesting is that the battle over an employer's legitimate interest in an employee's use of social media is also being played out among employees who are relatively junior within organizations and may, justifiably or unjustifiably, believe that their actions are not under the gaze of their employers.

This article compares the results of two recent cases from the United States and the United Kingdom with an earlier case from Canada.

Don't Make Fun of the Customers

In a recent U.S. National Labor Relations Board ("NLRB") decision, *Karl Knauz Motors, Inc. (Re)*,[1] the NLRB considered whether a car dealership could terminate a salesperson for comments on Facebook about an accident that involved a customer of the dealership. The customer had driven into a pond, and the salesperson posted photos on Facebook with sarcastic comments. The employer argued that the comments violated employee handbook rules that required employees to be "courteous, polite, and friendly to our customers, vendors and suppliers, as well as to their fellow employees" and that prohibited conduct that was "disrespectful" or involved the "use of profanity or other language which injures the image or reputation" of the employer.[2] In addition, not long before the post about the customer, the same salesperson had posted photos and comments criticizing food that had been served at a sales event at the dealership. The tenor of the earlier post was that the dealership should have served better food, given the profile of the sales event.

The salesperson claimed that he was terminated in violation of the protections afforded by s. 7 of the *National Labor Relations Act* [*NLRA*] that, among other things, provides salespersons with rights to participate in concerted activity for the purpose of collective bargaining and other mutual aid or protection.[3] The NRLB has previously issued decisions and guidance documents this year, warning that social media policies must not stifle workers from communicating about workplace conditions as this would offend s. 7 of the *NLRA*.[4]

An administrative law judge concluded[5] that the postings about the car accident did not fall within s. 7 of the *NLRA* because it was posted by the employee on his Facebook page and no discussion took place on Facebook about the post. By contrast, the comments about the food at the sales event were made in the context of an exchange among employees on Facebook. The administrative law judge concluded that the comments were related to the dealership's image at the event and this could affect the working conditions of the employees by affecting sales.

In a split decision, the NLRB upheld the decision of the administrative law judge. The employee's termination for the comments about the customer was not protected by the *NLRA*. However, the NLRB ordered that the employee handbook rules were overbroad and not enforceable.

The dissenting NLRB member concluded that the requirement to be courteous did not violate s. 7 of the *NLRA* and held that:

> [r]easonable employees know that a work setting differs from a barroom, room and they recognize that employers have a genuine and legitimate interest in encouraging civil discourse and non-injurious and respectful speech.[6]

Say What You Will About Gay Marriage

In *Smith v. Trafford Housing Trust*,[7] a housing manager of the Trust read a news article online regarding gay marriage and posted the link to his Facebook account with the comment "an equality too far."[8] The manager's Facebook privacy settings had been set so that his posting could be viewed by his "Friends" and also "Friends of Friends."[9] This prompted an exchange with one of the employee's colleagues at work, which was quite tempered but suggested that those gays and lesbians "have no faith and don't believe in Christ."[10] The employee was suspended and subjected to a disciplinary proceeding that resulted in a finding of gross misconduct. The employee was offered a demotion to a non-managerial position in view of the length of his service.

According to the decision of the England and Wales High Court of Justice (Chancery Division), the Trust had over 300 employees.[11] The court found that, at the material time, the employee listed that he was a manager at the Trust. His profile stated "What can I say—it's a job and it pays the

bills."[12] He described his religious views as "full on charismatic Christian."[13] His profile and wall pages also listed that he was a manager at the Trust. In putting the post into context, the court held that it was one of a number of posts about "sport, food, motorcycles and cars."[14]

The court concluded that a reasonable reader of the manager's wall would not have understood him to be a spokesperson for the Trust.[15] The court rejected that any loss of reputation by the Trust would arise in the mind of a reasonable reader. The manager's Facebook wall "was primarily a virtual meeting place at which those who knew of him, whether his work colleagues or not, could at their choice attend to find out what he had to say about a diverse range of non-work related subjects."[16] The court minimized the broader access to his wall by "friends of friends" by stating that "actual access would still depend upon the persons in that wider circle taking the trouble to access it."[17] The court found that the manager did not thrust his views onto colleagues at the office.[18] The medium and context was not "inherently" work related—just the opposite; it was inherently non-work related.[19] In the result, the court concluded that the manager had been constructively dismissed as the Trust had not been entitled to discipline the manager.

Don't Diss and Threaten Other Employees or Your Employer

The problems for the employees in *Lougheed Imports Ltd. (West Coast Mazda) v. United Food and Commercial Workers International Union, Local 1518*[20] started when one of the employees posted on Facebook a message that could be interpreted as threatening: "Sometimes ya have good smooth days when nobody's [*expletive*] with your ability to earn a living … and sometimes accidents DO happen, its [*sic*] unfortunate but thats [*sic*] why there [*sic*] called accidents right?"[21] Another employee also was posting derogatory comments about managers and the company.[22]

The first employee had close to 100 "friends," and the second employee had approximately 377 "friends."[23] Significantly, the posts were escalating in tone. They were so extreme that one person "defriended"[24] and the girlfriend of one of the employees commented that "[s]omethings [*sic*] just shouldn't be broadcasted on facebook, especially when you still work there."[25]

After a series of confrontations with the employees about their conduct, the employer eventually terminated the employment of the two employees. The union grieved but lost. In an interesting counterpoint to the *Trafford Housing Trust* case, the British Columbia Labour Relations Board concluded that the comments on Facebook had sufficient proximity to the employer's business. The comments had been used as a "verbal weapon."[26] They went beyond shop floor comments to insubordination in front of employees who were friends of the employees by degrading a manager and referring to discipline.[27] In the result, the termination was upheld.

Substance, Purpose, and Context

Of course, one should be careful to draw conclusions from a small sample of cases crossing multiple jurisdictions, each with its own approach to employment and privacy laws. However, one theme that emerges in all three cases is that, in addition to the substance of the social media posts, the purpose and context for those postings are important considerations in concluding whether the employer has a legitimate interest in the employee's social media activities.

---

1 2012 NLRB Lexis 679.

2 *Ibid*. at *1.

3 29 U.S.C. 157.

4 *Costco Wholesale Corporation (Re)*, 2012 NLRB Lexis 534. NLRB Operations Memorandum 12-59 (May 30, 2012), <http://mynlrb.nlrb.gov/link/document.aspx/09031d4580a375cd>; NLRB Operations Memorandum 12-31 (January 24, 2012), <http://mynlrb.nlrb.gov/link/document.aspx/09031d45807d6567>; NLRB Operations Memorandum 11-74 (August 18, 2011), <http://mynlrb.nlrb.gov/link/document.aspx/09031d458056e743>.

[5] *Supra* note 1 at *22 *et seq*.
[6] *Ibid*.at *12.
[7] 2012 EWHC 3221 (Ch).
[8] *Ibid*. at para. 1.
[9] *Ibid*. at para. 29.
[10] *Ibid*. at para. 4.
[11] *Ibid*. at para. 12.
[12] *bid*. at para. 31.
[13] *Ibid*.
[14] *Ibid*. at para. 33.
[15] *Ibid*. at para. 57.
[16] *Ibid*. at para. 76.
[17] *Ibid*.
[18] *Ibid*.
[19] *Ibid*. at para. 75.
[20] [2010] B.C.L.R.B.D. No. 190.
[21] *Ibid*. at para. 13.
[22] *Ibid*. at paras. 37–38.
[23] *Ibid*. at para. 67.
[24] *Ibid*. at paras 21–22.
[25] *Ibid*. at para. 40.
[26] *Ibid*. at para. 98.
[27] *Ibid*.

INVITATION TO OUR READERS
Do you have an article that you think would be appropriate for *Canadian Privacy Law Review* 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 *Canadian Privacy Law Review*?

If so, please feel free to contact Michael A. Geist
@mgeist@uottawa.ca
OR
cplr@lexisnexis.ca