

2011-04 — Information & Technology Law Newsletter

Date: October 2011

Contents

- I. Articles
 - I.1 Canada's Anti-spam Legislation Enacted and Public Consultation Open for Draft Regulations
- II. Case Comments
 - II.1 *R. v. Tuduce*, 2011 ONSC 2749
 - II.2 Text is Not Talk: *R. v. Telus Communications Co.* (2011), 2011 CarswellOnt 1331, 2011 ONSC 1143 (Ont. S.C.J.)
 - II.3 *Walsh v. R.* (2011), 2011 CarswellNat 3191, 2011 TCC 341 (T.C.C. [Informal Procedure])
 - II.4 *Velsoft v. GlobalA* Nebulous Anton Piller Order Condition Strictly Applied
 - II.5 *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2011 SCC 25
 - II.6 *Martinek v. Dojc et al.* Ont S.C.T.J., Divisional Court, June 27, 2011
- III. Case Digests
 - III.1 *Abougoush v. Sauve* (2011), 2011 BCSC 885, 2011 CarswellBC 1712 (B.C. S.C.)
 - III.2 *R. v. Skakun* (2011), 2011 BCPC 98 (B.C. Prov. Ct.)

I. — Articles

I.1 — Canada's Anti-spam Legislation Enacted and Public Consultation Open for Draft Regulations

J. Andrew Sprague Miller Thomson LLP

Anti-spam Legislation Enacted

Canada's anti-spam legislation (the "Act" or "CASL")¹ was enacted on December 15, 2010. The Act regulates a broad range of activities, including the sending

¹The official name of the legislation is "An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act".

of commercial electronic messages, the altering of transmission data, and the use of spyware.²

Subject to certain exceptions, the Act prohibits a sender from transmitting a commercial electronic message to an electronic address, unless: (i) consent to send has been obtained from the individual associated with the electronic address; and (ii) certain requirements to include information in the message are met.

A request for express consent must set out the purposes for which consent is sought and meet certain requirements as to the information to be included. The draft regulations discussed below describe the information requirements.

The Act also sets out circumstances in which consent to the sending of messages may be implied. For example, implied consent may arise based on an existing business relationship or an existing non-business relationship.

An existing “business relationship” will arise based on the purchase or lease of a product or service, the acceptance of an investment opportunity or the making of a contract, in each case within two years prior to the sending of a message.

Section 10(13) of the Act sets out several circumstances in which two persons will be deemed to have an “existing non-business relationship”, such that consent for the sending of unsolicited commercial electronic messages will be implied. One such instance is where a club, association or voluntary organization (a “CAVO”) sends a commercial electronic message to a person who is or was a member of such CAVO within the preceding two-year period.

Public Consultation Open for Draft Regulations

Recently, the federal government released for public consultation two different sets of draft regulations under the Act. The first set was released by the Canadian Radio-television and Telecommunications Commission (“CRTC”) on June 30, 2011, and the second set was released by the Department of Industry on July 9, 2011.

Comments on the draft regulations are being sought by both the CRTC and the Department of Industry.

The draft CRTC regulations (the “CRTC Regulations”) and details on how to provide comments to the CRTC are available at: <http://www.crtc.gc.ca/eng/archive/2011/2011-400.htm>. Individuals who are interested in commenting on the draft CRTC Regulations must do so by **August 29, 2011**.

The draft Department of Industry regulations (the “Industry Regulations”) and details on how to provide your comments to the Department of Industry are

²More information on the Act can be found in Roxanne Chow’s article entitled “Bill C-27 vs. Bill C-28: Canada’s Proposed Fighting Internet and Wireless Spam Act”, which appeared in the April 2010 issue of this publication.

available at: <http://www.gazette.gc.ca/rp-pr/p1/2011/2011-07-09/html/reg1-eng.html>. Individuals who are interested in commenting on the draft Industry Regulations must do so by **September 7, 2011**.

It is expected that the Act and the regulations will come into force this fall.

Overview of Draft Regulations

Information Required in Commercial Electronic Messages

Under the draft CRTC Regulations, all commercial electronic messages that are covered by the Act must contain information about the name of the person sending the message, and any other person on whose behalf the message is sent; any different name(s) by which such persons carry on business; and the physical and mailing address, telephone number (which includes access to an agent or voice message system), email address and web address of such persons.

In recognition that it may not be practicable to include the above noted information within a commercial electronic message, the draft CRTC Regulations provide an alternative mechanism whereby such information may be provided by a clear and prominent link to a web page.

Consent Required for Altering Transmission Data and Installing Programs

The draft CRTC Regulations also make the requirements for requesting consent to send commercial electronic messages applicable to requests for consent relating to the alteration of transmission data and the installation of computer programs. A separate request for consent is required for each such act, as is the inclusion of a statement indicating that any of the means of contacting the sender described in subparagraph (c) of the preceding section may be used to withdraw consent.

If a request for consent relates to the installation of a computer program, under the draft CRTC Regulations, the program's material elements that perform one or more of the functions listed in subsection 10(5) of the Act must be set out apart from other information in the request and brought to the attention of the recipient of the request. As well, the person providing consent must acknowledge in writing that they understand and agree that the program performs the specified functions.

Personal Relationship and Family Relationship

The draft Industry Regulations set out the meaning of a "family relationship" and a "personal relationship". If either type of relationship exists between the sender and the recipient, messages between them, including commercial electronic messages, are not required to comply with the Act.

A "family relationship" means the relationship between two individuals who are connected by: (a) a blood relationship; (b) marriage; (c) a common-law partnership; and (d) adoption. Each of the four classes is further defined within the draft Industry Regulations.

A "personal relationship" means the relationship, other than in relation to a commercial activity (as defined in the Act), between the sender and recipient of a

message, if they have had an in-person meeting and, within the previous two years, a two-way communication.

Conditions for Use of Consent

Section 10(2) of the Act provides that a person may seek consent for any activities set out in the Act on behalf of a person whose identity is not disclosed provided that the person seeking consent complies with the requirements in the regulations.

The draft Industry Regulations permit a person who obtained express consent from an intended recipient on behalf of an unknown person to authorize any sender to rely on the consent, provided that certain criteria, as set out in the draft Industry Regulations, are complied with. These criteria address, in part, requirements relating to the withdrawal of consent.

Membership in a Club, Association and Voluntary Organization

For purposes of the provisions of the Act permitting messages to be sent by a CAVO to a member, the draft Industry Regulations define “membership” as the status of having been accepted as a member of a CAVO in accordance with its membership requirements. The draft Industry Regulations also define a “club, association or voluntary organization” as a non-profit organization that is organized and operated exclusively for social welfare, civic improvement, pleasure or recreation or for any purpose other than profit, if no part of its income is payable to, or otherwise available for the personal benefit of any proprietor, member or shareholder of that organization, unless the primary purpose of the organization is the promotion of amateur athletics in Canada.

II. — Case Comments

II.1 — R. v. Tudeau, 2011 ONSC 2749

Gregory Cohen Miller Thomson LLP

Background

This was an application by Adrian Tudeau (“Tudeau”) pursuant to s. 24 of the *Charter of Rights and Freedoms* for an order to exclude evidence found during police searches.

In 2009, Tudeau was stopped by a police officer for speeding. His driver’s license had been suspended a month earlier. He was placed under arrest and searched. There was an initial search of the car, followed by a second search of the car after it was impounded. The searches revealed that Tudeau was in possession of identification records, credit cards and debit cards in various names, together with card programming equipment, and a USB memory stick without password protection. The memory stick was subsequently examined by a Technical Crimes Unit member. The four searches were conducted without a warrant.

It is worth noting that at the time of the incident search warrants were not needed to examine the content of electronic items seized during a search in rela-

tion to an arrest, but this has since changed. A search warrant would be required now.

Decision

Tuduce argued that all four of the warrantless searches were prima facie unreasonable, and the Crown had the onus to prove on a balance of probabilities that each search was reasonable.³ The Court found, however, that only the search of the memory stick was unreasonable. The examination of electronic content encompassing vast amounts of sensitive, personal, private, and confidential information could not be justified without a warrant.

4

Section 24(2) of the *Charter* provides for the exclusion of evidence that would bring the administration of justice into disrepute. A three-part process was used by the Court when responding to the question of whether evidence disclosed from the search of the memory stick should come within the exclusion. The Court considered:

- the seriousness of the infringing state conduct;
- the impact of the breach on the accused's interests; and;
- society's interest in the adjudication of the matter.

In assessing the seriousness of the infringing conduct, the Court took into consideration Tuduce's reasonable expectation of privacy with respect to the data. The fact that the data on the memory stick was not password-protected suggested a lesser expectation of privacy. As such, Justice Taylor found that the reputation of the justice system would not be brought into disrepute as a result of the admission into evidence of the information disclosed from the search of the USB memory stick.

Conclusion

A person can reasonably expect a higher level of privacy and the protection afforded by the *Charter* if the devices on which personal data is stored are protected by encryption and other security measures. For purposes of any possible intrusion by state actors and the protection granted under the *Charter*, the use of encryption for the protection of data on electronic devices is analogous to the use of locks on doors to one's personal residence.

³s.495 (1)(a) of the *Criminal Code* was amended to change the words reasonable and probable grounds to reasonable grounds. The Supreme Court explained that something may be reasonable but not probable to occur. In other words, 'not unlikely to occur for reasons that rise above a mere suspicion' (*R. v. Mann* (2004), [2004] S.C.J. No. 49, 2004 CarswellMan 303 (S.C.C.)).

⁴*R. v. Polius* (2009), 2009 CarswellOnt 4213, [2009] O.J. No. 3074 (Ont. S.C.J.); *R. v. Manley* (2011), 2011 CarswellOnt 803, 2011 ONCA 128, [2011] O.J. No. 642 (Ont. C.A.) at para. 39.

II.2 — Text is Not Talk: R. v. Telus Communications Co. (2011), 2011 CarswellOnt 1331, 2011 ONSC 1143 (Ont. S.C.J.)

Elisabeth Symons Miller Thomson LLP

Background

Telus Communications Company (“Telus”) received a General Warrant and Assistance Order (the “Warrant”). Unlike most warrants which seek the production of existing information, the Warrant sought information on a going-forward basis. Beginning on a set date and continuing for a period of 14 days, Telus was obliged to provide on a daily basis the following information relating to two of its subscribers: (i) all text messages sent or received; and (ii) all related subscriber information for senders and recipients. Telus challenged the Warrant, and the Crown sought to uphold it.

Arguments

Telus argued that: (i) the Warrant was not the correct form of warrant or order for authorizing the interception of private communications; (ii) a going-forward warrant should not be available when a traditional retrospective warrant would be sufficient; (iii) given the high expectation of privacy that exists in relation to text messages, requiring law enforcement to obtain an authorization similar to the authorization required for a wiretap would be in the best interests of the administration of justice; and (iv) the cost and inconvenience of performing the manual tasks necessary to comply with the Warrant make doing so unworkable.

The Crown argued that: (i) Telus would not be intercepting private communications as they occurred, because text messages could be retrieved from the servers on which they were stored rather than being intercepted in real time; (ii) the ongoing collection of information would not have been possible or reasonable with a more traditional retrospective warrant; and (iii) neither cost nor inconvenience are grounds to set aside a warrant that the *Criminal Code*⁵ permit the police to obtain.

Background

Text messages are short text-based messages sent to a cellular device such as cellular phone or a smart phone. They are also typically sent from cellular devices, but can also be sent from any device capable of browsing on the Internet. Text messages can only be delivered when the cellular device is turned on and has service, failing which the applicable cellular provider for the receiving device will retain the text message until it can be delivered.

General warrants to use any investigative technique or device for a set purpose (such as the Warrant) are issued under section 487.01 of the *Criminal Code*, and

⁵R.S.C., 1985, c. C-46

are available only if no other type of warrant can be used to achieve the same end.

Decision

On the interception issue, Sproat J. concluded that the Warrant did not authorize the interception of private communications because: (i) the plain meaning of the word “intercept” requires a real-time capture of the messages, which was not what was contemplated by the Warrant; (ii) it is not logical to determine whether or not a communication has been “intercepted” according to whether it was delivered to someone before being turned over to the police; and (iii) it is the responsibility of Parliament to determine whether or not records of text messages should be treated more like telephone conversations (i.e. private communications) and less like business records for the purposes of warrants. As Telus was in the practice of storing all text messages sent or received over its system on any day for a period of 30 days by copying each one to a database, Sproat J. did not make any finding as to whether or not retrieving messages from storage intrinsic to the communication process would be an interception.

On the question of whether or not a more traditional warrant should have been used, Sproat J.: (i) noted that courts should take into account the fact that a section 487.01 general warrant is intended to be a flexible tool when determining whether an alternate investigative tool could be used; (ii) acknowledged that the same information obtained under the Warrant (a general warrant) could have been obtained by the police by using 14 separate warrants (i.e. one for each day); and (iii) concluded that it was impractical to expect the police to obtain separate warrants for each of 14 days with respect to the information sought under the Warrant.

On the issue of whether or not an individual’s expectation of privacy with respect to his or her text messages is sufficiently high that it was in the best interests of the administration of justice to require the police to obtain an authorization similar to that required for a wiretap when they seek access to an individual’s text messages, Sproat J. concluded that it was the responsibility of Parliament to decide this issue.

Sproat J. also concluded that cost and inconvenience are merely two factors that a judge may take into account when determining whether or not to issue a general warrant, but noted that costs should be expected to be incurred in the course of assisting law enforcement.

Conclusion

It would have been helpful if the decision had ventured an opinion, even in obiter, about whether or not a text message should be treated more like private conversations rather than business records, but the decision on Sproat J.’s part not to do so is understandable. Various efforts have been made in the past 15 years in Canada to enact legislation relating to lawful access. Such efforts have stirred up strongly held opposing beliefs about the extent to which it is appropri-

ate and reasonable to require telecommunications companies to retain information about messages sent and received by their subscribers, and the conditions under which such companies should be required to provide that information to law enforcement.

II.3 — Walsh v. R. (2011), 2011 CarswellNat 3191, 2011 TCC 341 (T.C.C. [Informal Procedure])

Meg Spevak Miller Thomson LLP

This appeal relates to a reassessment made under the *Income Tax Act* denying the Appellant (Walsh) the right to claim business losses in 2005 and 2006 on the basis that they were personal expenses.

In 2005, Walsh acquired trading software and a computer on which to run the software in order to start a new business. The software provided training in trading activities and on-line daily support with demonstration trading accounts. He also joined a user group for the software.

Walsh prepared books and accounts for his business, and filed a statement of business activities with his 2005 and 2006 returns with the Canada Revenue Agency (“CRA”).

Decision

The Court was not satisfied that Walsh was undertaking anything other than a training program for the two years in question, as his testimony underlined that the focus of his activity was conducting research and learning the market in order to exploit it.

Relying on the 2002 Supreme Court of Canada decision in *Stewart v. Canada*⁶, the Respondent took the position that the activity of developing the know-how to operate a specific type of business (which was the Appellant’s intention) is a form of personal development, rather than a commercial activity *per se*. Indicia of commerciality must be sufficient to warrant a finding that there is a source of income.

The Court agreed with the Respondent that the Appellant’s activities in 2005 and 2006 were not a means for earning income and did not reach the level of commerciality to justify a finding that a business had commenced. Further, the Court stated that engaging in educational programs in preparation for the commencement of a business is essentially a personal rather than a business activity. Based on all the evidence, the appeal was dismissed.

II.4 — Velsoft v. GlobalA Nebulous Anton Piller Order Condition Strictly Applied

Karen Durell Miller Thomson LLP

⁶*Stewart v. R.* (2002), 2002 SCC 46, 2002 CarswellNat 1070 (S.C.C.)

A recent case heard by the Supreme Court of Nova Scotia articulates and supports the legal tenet that an *Anton Piller* order is an “exceptional remedy” which will be granted only on rare occasions. Justice McDougall, speaking in *Velsoft Training Materials Inc. v. Global Courseware Inc.*⁷, particularly highlighted the importance of establishing one of the conditions required for granting an *Anton Piller* order, namely, the need to demonstrate a “real possibility” that the defendant may destroy material before the discovery process. The difficulty in satisfying this condition is one of the reasons why the remedy is rarely applicable.

Four Conditions for Grant of Anton Piller Order

Justice McDougall recognizes that this requirement is only one of four “essential conditions for the making of an Anton Piller order”. All four conditions are set out in the authoritative decision of *Celanese Canada Inc. v. Murray Demolition Corp.*⁸. Justice Binnie held in that case that an Anton Piller order will be granted only if the plaintiff establishes: (i) a “strong prima facie case”; (ii) serious (either potential or actual) damage to the plaintiff due to the defendant’s alleged misconduct; (iii) “convincing evidence” that the defendant is in possession of “incriminating documents, or things”; and (iv) a “real possibility” of destruction of materials.

Possibility of Destruction of Materials

In the *Velsoft* case Justice McDougall determined that three of the four conditions were met by the plaintiff, but that the *Anton Piller* order previously imposed should be set aside due to the failure of the plaintiffs to adduce evidence of a real possibility of the destruction of materials.

Justice McDougall noted that an *Anton Piller* order is more than “simply an alternative method of making disclosure”, but instead, is “intended to prevent the loss or destruction of evidence.” It is an obvious conclusion that if the nature of such an order is to prevent destruction of evidence, proof of the intention to destroy evidence must be shown in order for the order to be imposed.

The plaintiffs in the *Velsoft* case demonstrated multiple instances of conduct indicating that the defendants would destroy evidence if the order were not imposed. Firstly, they established that one of the defendants had forensically wiped clean a computer before returning it to the plaintiffs, notwithstanding that no instructions had been provided to the defendant to take this action. Secondly, the plaintiffs alleged that employment contracts, to which the same defendant had exclusive access, went missing, with the reasonable inference being that the defendant took such documents. Thirdly, the plaintiffs alleged that the same defendant and other defendants engaged in business dealings in direct competition with the plaintiff while still employed by the plaintiff. The plaintiffs suggested

⁷(2011), 2011 CarswellNS 463, 2011 NSSC 274 (N.S. S.C.).

⁸(2006), [2006] 2 S.C.R. 189 (S.C.C.) , at para. 15.

that this evidence pointed to a propensity and interest on the part of the defendants to destroy materials.

Justice McDougall agreed with prior jurisprudence which found that clear, indisputable evidence that a defendant is arranging in advance to destroy materials is unlikely to be available to a court in a case in which an *Anton Piller* order is sought. While recognizing that this condition can be difficult to prove, Justice McDougall upholds the requirement that persuasive evidence must be stronger than merely showing that a defendant has “engaged in questionable business practices in the past”, or is “generally dishonest”. The requisite standard is evidence showing a “grave danger” and a “real possibility” that materials may be destroyed or otherwise hidden prior to a discovery process.

Comments and Conclusions

The imposition of an *Anton Piller* order can have serious results. Canadian jurisprudence identifies *Anton Piller* orders as “very invasive”, and acknowledges that such orders can diminish the reputation of a defendant within his community. Justice McDougall reflects a prudent approach in stating that a finding that a defendant will destroy materials must be the result of a “stringent review”.

The *Vesloft* decision stands as a testament to the importance of each of the conditions required before an *Anton Piller* order will be granted by a Canadian court. In particular, any evidence to be adduced to show that materials will be destroyed must show a propensity of the defendants to take this step. The *Vesloft* decision demonstrates that the nebulous nature of the condition of a “real possibility” of destruction of materials should not be interpreted as lessening its importance as a step towards the grant of an *Anton Piller* order.

11.5 — Canada (Information Commissioner) v. Canada (Minister of National Defence), 2011 SCC 25

Roxanne Chow Miller Thomson LLP

This recent decision of the Supreme Court of Canada affirms the courts’ sensitivity to the separation of powers between the executive, legislative and judicial branches of government.

Background

Several access to information requests were made in 1999 and 2000 under the *Access to Information Act* (“Act”).⁹ These include requests made to the Department of National Defence for the minutes of the management meetings held in 1999 by the former Minister of National Defence, Art Eggleton, and senior staff from the Minister’s office (“M5 meetings”); the Privy Council Office and the RCMP for the daily agenda books of the Prime Minister between January 1994 to the present; and to the Department of Transport for a copy of the Minister of

⁹R.S.C. 1985, c. A-1.

Transport's itineraries and meeting schedules between June and November 1999.

When these offices did not provide the requested records, the Information Commissioner of Canada ("Commissioner") launched an investigation and concluded that the respective offices did in fact have copies of these records, and that certain pages of these records should be released. The offices refused to comply, leading the Commissioner to apply for judicial review.

Kelen J. of the Federal Court of Canada dismissed most of the requests for access, but allowed in part the requests made to the Department of National Defence for documents from the M5 meetings, as well as certain pages of the Prime Minister's agendas held by the Privy Council Office and the RCMP.¹⁰ The Federal Court of Appeal then overturned Kelen J.'s order to disclose the Prime Minister's agendas and dismissed the other appeals,¹¹ leading the Commissioner to appeal to the Supreme Court of Canada (the "Supreme Court").

Issues and Analysis

The Supreme Court considered three issues.

I. Is the Office of the Prime Minister, or a Minister, a 'government institution' within the meaning of the Access to Information Act?

Section 4(1) of the Act reads:

Subject to this Act, but notwithstanding any other Act of Parliament, every person who is

(a) a Canadian citizen, . . .

has a right to and shall, on request, be given access to any record under the control of a government institution.

¹⁰*Canada (Information Commissioner) v. Canada (Minister of National Defence)* (2008), [2009] 2 F.C.R. 86, 2008 FC 766, 2008 CarswellNat 1979 (F.C.), later appeal (2009), 2009 CarswellNat 2772 (S.C.C.).

¹¹*Canada (Information Commissioner) v. Canada (Minister of National Defence)* (2009), 2009 FCA 181 (F.C.A.) (CanLII), application/notice of appeal (2009), 2009 CarswellNat 2773 (S.C.C.), application/notice of appeal (2009), 2009 CarswellNat 2774 (S.C.C.), leave to appeal allowed (2009), 403 N.R. 398 (note), 2009 CarswellNat 4316 (S.C.C.), leave to appeal allowed (2009), 403 N.R. 398 (note), 2009 CarswellNat 4318 (S.C.C.), affirmed (2011), 331 D.L.R. (4th) 513, 416 N.R. 105, [2011] S.C.J. No. 25, [2011] 2 S.C.R. 306, 2011 CarswellNat 1474, 2011 CarswellNat 1475, 2011 SCC 25, 18 Admin. L.R. (5th) 181 (S.C.C.); and *Canada (Information Commissioner) v. Canada (Minister of National Defence)* (2009), 2009 CarswellNat 1521, 2009 FCA 175 (F.C.A.), application/notice of appeal (2009), 2009 CarswellNat 2772 (S.C.C.), application/notice of appeal (2009), 2009 CarswellNat 2775 (S.C.C.), leave to appeal allowed (2009), 403 N.R. 398 (note), 2009 CarswellNat 4314 (S.C.C.), leave to appeal allowed (2009), 403 N.R. 398 (note), 2009 CarswellNat 4320 (S.C.C.), affirmed (2011), 331 D.L.R. (4th) 513, 416 N.R. 105, [2011] S.C.J. No. 25, [2011] 2 S.C.R. 306, 2011 CarswellNat 1474, 2011 SCC 25, 18 Admin. L.R. (5th) 181 (S.C.C.).

The Supreme Court agreed with Kelen J.'s interpretation of this section, concluding that the ministerial offices are not part of the "government institution" for which they are responsible. The meaning of "government institution" is clear, and the omission of these ministerial offices from the list found in Schedule I of the Act demonstrates that Parliament did not intend for them to be considered as "government institutions".

II. Are the records requested, despite their physical location in the respective ministerial offices, "under the control" of the related government institution within the meaning of section 4 of the Access to Information Act?

Although the ministerial offices were not "government institutions", the Supreme Court went on to consider the two-part test for determining whether records are within the "control" of a government institution within the meaning of s. 4(1) of the Act.¹² The Court concluded that none of the requested records was in the control of a government institution. The Court also noted that the availability of judicial review and the Commissioner's investigatory powers under the Act are sufficient to facilitate an individual's right to access information, and therefore a presumption that Minister's records are within the scope of the Act "would dramatically expand the access to information regime in Canada"¹³.

Lebel J. disagreed with the majority's view on the latter point. The two-part "control" test must also consider that Ministers not only are members of Cabinet and accountable for the administration of a government department, but also are Members of Parliament, members of a political party and private individuals. Given the many roles and responsibilities of a Minister, the records associated with a Minister's office may fall under different categories, and there should not be a blanket presumption that a Minister's records are beyond the scope of the Act. There must be balance between government accountability and efficient governance.

III. Are the Prime Minister's agendas at issue exempt or excluded from disclosure pursuant to section 19 of the Access to Information Act and section 3(j) of the Privacy Act?

Although the Prime Minister's agendas in the possession of the RCMP and the Privy Council Office may be subject to disclosure insofar as they are under the

¹²The two-step test for "control" within the meaning of s. 4(1) of the Act considers the following:

- i. whether the record relates to a departmental matter; and
- ii. if the record requested does relate to a departmental matter, whether the government institution could reasonably expect to obtain a copy of the record, taking into consideration the substantive content of the record, the circumstances in which it was created, and the legal relationship between the government institution and the record holder.

¹³At para. 13.

control of a “government institution”, the disclosure of such records is subject to certain statutory exemptions. Section 19(1) of the Act prohibits the head of a government institution from releasing any record that contains “personal information”, as that term is defined in section 3(j) of the Privacy Act¹⁴. However, that section creates an exception that allows for the disclosure of information that pertains to an individual who is or was an officer of a government institution, and that relates to the position or function of the individual.

The Supreme Court concluded that Kelen J. erroneously relied upon the definitions of public officer found in the *Financial Administration Act* and the *Interpretation Act* in holding that the Prime Minister was an officer of Privy Council Office. Absent an express statement by Parliament, it would be inconsistent with Parliament’s intention to interpret the Privacy Act in a way that would treat the Prime Minister as an “officer” of the Privy Council Office. Thus, the Prime Minister’s agendas should not be disclosed, as the exception in section 3(j) of the Privacy Act does not apply.

Conclusion

In dismissing the appeal, the Supreme Court of Canada reiterated the concern expressed in decisions of the lower courts that a statute should not be interpreted in a manner that goes beyond the scope of the intention of Parliament in the enactment of the legislation. Once again, the courts remind us that judicial powers should not extend beyond the boundaries set up to maintain balance between the judiciary, on the one hand, and the executive and legislative branches of government, on the other hand.

II.6 — Martinek v. Dojc et al. Ont S.C.T.J., Divisional Court, June 27, 2011

J. Fraser Mann Miller Thomson LLP

The decision in the above-mentioned case provides insight into the meaning of “publication” of defamatory comments for purposes of the dissemination by means of the Internet.

Facts

The appellant had brought a claim for defamation based on the comments that had been posted by the respondent to a Yahoo! group called “Reunion”. The group was formed to allow for communication among persons with a shared background of Slovak or Czech and Jewish descent. Access to the user group was restricted to its members to whom a password had been assigned.

The appellant was a member of the group, but was excluded from membership as a result of a dispute arising from the conduct of one member. The appellant nevertheless gained access to the site by obtaining a password from a member in

¹⁴RSC 1985, c. P-21.

good standing. The appellant brought an action for defamation based on certain comments that had been posted to the group web-site.

Findings

The trial judge found that the allegedly defamatory comments were made without malice and were protected by qualified privilege. However, the Divisional Court found that this defence had not been pleaded by the respondent, and that the applicant should have been provided with an opportunity to dispute the application of the defence. On this basis, the Court found that the matter should be sent back for re-trial.

The Divisional Court also considered two additional issues raised in the appeal: first whether the material in question was “published” when it was circulated to a limited and private group, for which a password was required in order to gain access to the site; and second, whether the appellant was precluded from relying on documents posted on the site to assert a claim of defamation when he appeared to be a “trespasser” who had gained access to the site by being provided with a password assigned to another individual.

On the first question, the Divisional Court noted that the trial judge had made a finding that the Internet user group in question was a “closed, unpublished environment”, without having addressed the meaning of the legal requirements for messages to be published to a third party in order for the messages to be defamatory. The Court found that since the law of defamation in the context of the Internet is still under development, it was necessary to consider the question of whether the posting of comments to a closed site could constitute defamation based on a review of all factual circumstances.

The Court also noted that there did not appear to be any case law which precluded a plaintiff from advancing a claim for defamation based on the manner in which the plaintiff became aware of the claim. Moreover, since the plaintiff raised questions as to whether he was in fact a “trespasser” to the site, it was necessary for a court to consider this issue in the context of a trial with a full factual record.

Comments

The decision leaves open for a new trial judge to consider, after a review of all relevant evidence, the question of whether the posting of comments to a closed user group may constitute “publication” for purposes of the law of defamation. The decision also leaves open the possibility that even where a claimant in a defamation case becomes aware of the alleged acts of defamation by obtaining unauthorized access to a web site, this fact by itself does not disentitle the individual from pursuing the claim.

III. — Digests

III.1 — Abougoush v. Sauve (2011), 2011 BCSC 885, 2011 CarswellBC 1712 (B.C. S.C.)

Nelly Mosstaghimi Miller Thomson LLP

Facts

The plaintiff alleged that she suffered injuries in a traffic accident which had a negative impact on her ability to function. She was unable to work or attend college classes. The defendants requested that photographs depicting the plaintiff's activities taken during a vacation after the accident be produced in discoveries since they were relevant to the question of the extent of her injuries and her ability to carry out various activities.

Decision

The judge reviewed all of the photographs and determined that: (i) they were relevant to the plaintiff's view of what is a physical activity and also to her tolerance for engaging in such activity over a several week period; and (ii) the photographs were not embarrassing to the plaintiff, nor did they show the plaintiff in socially unacceptable situations (noting that there was nothing in the photographs that would prevent the plaintiff from posting them on a social networking site or that would require them to be withheld from the defendants for privacy reasons).

Based on the foregoing, the judge ruled that the vacation photographs should be provided to the defendants, and in the interest of providing a complete record, that the metadata imbedded in the digital images should also be provided to the defendants. The metadata would include information about the date and time when a picture is taken as well as GPS co-ordinates for the location at which the picture was taken, which information is captured by some digital cameras.

III.2 — R. v. Skakun (2011), 2011 BCPC 98 (B.C. Prov. Ct.)

Meg Spevak Miller Thomson LLP

Facts

The Defendant was charged with a breach of section 30.4 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA")¹⁵ which states that an employee, officer or director of a public body must not disclose personal information except as is authorized by FIPPA.

The Defendant, a city councillor of the City of Prince George (the "City"), received a report in a closed, restricted city council meeting which contained personal information (as defined in FIPPA) about a number of persons. The Defen-

¹⁵R.S.O. 1990, c. F.31.

dant delivered the report to the Canadian Broadcasting Corporation (the “CBC”), and the report was subsequently published on the CBC website.

Arguments

The Defendant argued that: (i) FIPPA did not apply to city councillors insofar as they were not included in the term “officer” in section 30.4; (ii) the City failed to bring proceedings within the limitation period; and (iii) the “whistleblower” defence applied in this case.

Findings

The Court found that city councillors are officers of a public body for the purposes of FIPPA, and accordingly that the Defendant was an officer to whom FIPPA applied. The Court also found that the limitation period on the action had not expired since the information in the case was laid within one year following the date on which the Defendant delivered the report to the CBC. Further, the Court found that the “whistleblower” defence was not available to the Defendant since a charge under FIPPA is quasi-criminal, and the “whistleblower” defence is available only in civil and administrative employer/employee matters. By taking it upon himself to disclose the report to the media, the Defendant ignored the safeguards and protections afforded by FIPPA.

The Defendant was found guilty of breaching section 30.4 of FIPPA.