INTERNATIONAL ASSOCIATION OF YOUNG LAWYERS

IP/IT MEDIA & TELECOM - Workshop:

LONDON 2015

National Report for Canada

David Ma (dma@blaney.com / +1 (416) 596-2895)
Dina Maxwell (dmaxwell@blaney.com / +1 (416) 593-3949)[1]

Blaney McMurtry LLP
2 Queen St East, Suite 1500
Toronto, Ontario,
M5C 3G5
Canada

General Reporters:

Jerome Debras, Woog & Associés, Paris, France
jdebras@woogassocies.com

Cristina Hernandez-Marti Perez, Hernandez Marti Abogados, Barcelona, Spain
cristina@hernandez-marti.com

20 February 2015

[1] The authors gratefully acknowledge the work and support of Lisa Bruni, David Frank, Paul Pimentel, Simon Reis and Jodi Solomon, Articling Students at Blaney McMurtry, in the preparation of this report.

Table of Contents

1 Privacy Rights

1.1 Are privacy rights statutory rights or case-law based?

Privacy rights are based on both statutory law and case law. Privacy rights are statutory rights subject to judicial interpretation in case law. Various statutes cover privacy rights in the private and public sectors.

1.1.1 Statutes

1.1.1.1 Personal Information Protection and Electronic Documents Act

The *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*")[2] is a federal statute governing the collection and use of personal information from individuals by private-sector organizations. It applies to every organization that collects, uses or discloses personal information in the course of commercial activities.[3] "Organization" is defined to include an association, a partnership, a person and a trade union.[4] Personal information is defined as information about an identifiable individual.[5] Personal information does not include the name, title or business address or telephone number of an employee of an organization.[6] Commercial activity is defined as any particular transaction, act or conduct or any regular course of conduct that is of a commercial character.[7] The term "commercial character" is not defined. *PIPEDA* specifies that the selling, bartering or leasing of donor, membership or other fundraising lists is considered commercial activity.[8] The federal privacy commissioner has opined that "commercial activity" should be considered broadly to include any regular course of conduct that is of a commercial nature. *PIPEDA* also applies to personal information of employees of federally regulated works, undertakings or business.[9]

1.1.1.2 Scope of PIPEDA

Generally, *PIPEDA* does not apply to government institutions, or if the collection, use or disclosure of the personal information is strictly for non-commercial purposes. Furthermore, *PIPEDA* does not apply if a province has introduced "substantially similar legislation", in which case *PIPEDA* is displaced by the provincial legislation within that province. Substantially similar legislation to *PIPEDA* is generally defined as legislation that: (a) provides privacy protection that is consistent with and equivalent to that found under *PIPEDA*; (b) incorporates the ten principles in Schedule 1 of *PIPEDA* (see Appendix A); (c) provides for an independent and effective

[2] SC 2000, c 5 <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/>
[3] *Ibid*, s 4(1)(a).
[4] *Ibid*, s 2(1).
[5] *Ibid.*
[6] *Ibid.*
[7] *Ibid.*
[8] *Ibid.*
[9] *Ibid* at s 4(1)(a).

oversight and redress mechanism with powers to investigate; and (d) restricts the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.[10]

To date, Alberta, British Columbia, and Quebec have all passed substantially similar legislation, which will apply instead of *PIPEDA*, provided that the information is collected, used and disclosed entirely within that province.[11] These provinces have enacted the *Personal Information Protection Act*[12], the *Personal Information Protection Act*[13], and *An Act Respecting the Protection of Personal Information in the Private Sector*[14], respectively. Further, Manitoba's new *Personal Information Protection and Identity Theft Prevention Act* ("*PIPITPA*") received Royal Assent on September 13, 2013, but has not yet come into force.[15] It remains to be seen whether *PIPITPA* is substantially similar legislation to *PIPEDA*.

The provinces of Ontario, New Brunswick, and Newfoundland and Labrador have substantially similar legislation to PIPEDA only in respect of personal health information collected, used, or disclosed by custodians (*Personal Health Information Protection Act*[16] ("*PHIPA*"), *Personal Health Information Privacy and Access Act*[17], *Personal Health Information Act*[18], respectively). Under these statutes, rigorous requirements apply, including in Ontario, which imposes a duty on health information custodians to notify individuals of any breach in the use or disclosure of their personal information.

Some provinces and territories have also passed their own privacy laws with respect to personal health information, such as Prince Edward Island and Nova Scotia, which have not been declared substantially similar to *PIPEDA*. Therefore *PIPEDA* may still apply to health information in these provinces.[19]

1.1.1.3 Amendments to Alberta's Personal Information Protection Act

On December 17, 2014 Alberta's *Personal Information Protection Act* ("*PIPA*") was amended by Bill 3, in response to the Supreme Court of Canada's decision to strike down *PIPA* in *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*[20] *("United Food")*, on the basis that it infringed on the union's freedom of expression. Bill 3 amended *PIPA* to provide that during lawful labour disputes, a union is no longer required to obtain consent in order to collect, use, or disclose personal information, so long as certain conditions are met. The primary conclusion of the court was that "*PIPA* deems virtually all

---

[10] Office of the Privacy Commissioner of Canada, *Substantially Similar Provincial Legislation*, (March 22, 2013), < https://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp>.
[11] *Ibid.*
[12] SA 2003, c P-6.5.
[13] SBC 2003, c 63.
[14] RSQ, c P-391.
[15] Bill 211, SM 2013 c. 17, *The Personal Information Protection and Identity Theft Prevention Act*, <http://web2.gov.mb.ca/laws/statutes/2013/c01713e.php>.
[16] 2004, SO 2004, c 3, Sch A.
[17] SNB 2009, c P-7.05.
[18] SNL2008 c P-7.01.
[19] Office of the Privacy Commissioner of Canada, *Privacy Legislation in Canada*, (May 15, 2014), < https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp>.
[20] 2013 SCC 62.

personal information to be protected regardless of context."[21] To date, it is unclear whether or not the enactment of Bill 3 has rendered *PIPA* constitutional, as debates in the legislative assembly of Alberta suggest that Bill 3 has not addressed the underlying nature of the matters that the Supreme Court found unconstitutional in *United Food.*[22] Further, the constitutionality of *PIPA*, with respect to its provisions addressing labour disputes is unclear, because they have not yet been tested by the courts.

1.1.1.4 Federal Privacy Act

Various legislation protects privacy rights as between individuals and the government. The federal *Privacy Act*[23] restricts the collection, use and disclosure of personal information by federal government departments, ministries and agencies, including some federal Crown Corporations. Provinces and municipalities have passed similar legislation protecting persons from the disclosure of information held by those governments. For example, Part III of the Ontario *Freedom of Information and Protection of Privacy Act* ("*FIPPA*") contains laws which govern the collection, use, and disclosure of personal information, which apply to a range of provincial government institutions, including ministries and agencies, as well as educational institutions including universities and colleges.[24] Part II of the province's *Municipal Freedom of Information and Protection of Privacy Act* ("*MFIPPA*") contains similar laws regarding the handling of personal information by municipalities, school boards, police services boards, transit commissions and other municipal bodies.[25]

1.1.1.5 Constitutional Protection of Privacy Rights

Privacy rights between as between individuals and the government are also constitutionally protected. Section 8 of the *Canadian Charter of Rights and Freedoms* (the "*Charter*") provides that "everyone has the right to be secure against unreasonable search or seizure."[26] "This section has been judicially interpreted "to establish a right to privacy."[27] Section 2(b) of the *Charter*, which provides for freedom of expression, has also been judicially interpreted as a right to say nothing at all and therefore affords a privacy right.[28]

---

[21] *Ibid* at 25.
[22] Alberta, Legislative Assembly, Hansard, 28th Leg, 3rd Sess, No 10e (1 December 2014) at 259-265, <http://www.assembly.ab.ca/ISYS/LADDAR_files/docs/hansards/han/legislature_28/session_3/20141201_1930_01_han.pdf>. See also p. 262.
[23] RSC 1985, c P-21
[24] RSO 1990, c F.31, at s. 1, 2(1), 37-43.
[25] RSO 1990, c M.56, at s. 27-38.
[26] *The Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.
[27] *Canada (Director of Investigation & Research, Combines Investigation Branch) v Southam Inc.*, 1984 CarswellAlta 121, [1984] 2 S.C.R. 145, at 24-25.
[28] Peter Hogg, *Constitutional Law of Canada: 2011 Student Edition* (Toronto: Thomson Reuters, 2011) at 43-17 to 43-18 citing *RJR-MacDonald v Canada* (1995) [1995] 3 SCR 199.

1.1.2 Case Law

1.1.2.1 PIPEDA

Both the federal *Privacy Act* and *PIPEDA* provide a mechanism for a review of the government's access decision to an independent commissioner appointed under the statute. The Office of the Privacy Commissioner ("Commissioner") oversees *PIPEDA* and provides advice on how organizations may comply with their privacy obligations under the statute. Also, individuals may complain to the Commissioner about the personal information practices of organizations, or the Commissioner may initiate a complaint itself.[29]

The Commissioner's mandate includes public education and research into the protection of personal information.[30] The Commissioner has an ombudsman-like role through which non-binding recommendations are made and has broad investigatory powers, including the power to enter premises, to compel production of documents, and to summon and examine individuals under oath. At the conclusion of an investigation, the Commissioner may issue reports that contain findings and recommendations. These recommendations may be enforceable by way of an application to the Federal Court of Canada, as the Commissioner does not itself have order-making powers. The Federal Court of Canada has the authority to issue rulings and make orders under *PIPEDA*.[31] For a more detailed explanation on the powers of the Commissioner, please refer below to section 4.3.

Failure to comply, or a suspicion of non-compliance, with *PIPEDA* may result in (i) a Commissioner's investigation into or audit of an organization's personal information practices, (ii) a public report of the Commissioner detailing their investigation and findings, or (iii) litigation in the Federal Court of Canada with the prospect of fines, sanctions, and/or criminal liability.[32]

1.1.2.2 Tort of Intrusion Upon Seclusion

The Ontario Court of Appeal has recently recognized a relatively new tort of intrusion upon seclusion (i.e. invasion of privacy) in the case of *Jones v Tsige ("Jones").*[33] The Court formulated an objective standard for the new tort as follows:

> One who intentionally [or recklessly] intrudes, physically or otherwise, upon the seclusion of another or his [or her] private affairs or concerns, is subject to liability to the other for invasion of his [or her] privacy, if the invasion would be highly offensive to a reasonable person.[34]
>
> The key features of this cause of action are, first, that the defendant's conduct must be intentional, within which I would include reckless; second that the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and third,

[29] *Supra* note 2, s. 11.
[30] *Ibid* at s. 24.
[31] *Ibid* at s. 12-18.
[32] *Ibid* at s.18, 20(2), 14(1), 2(1).
[33] *Jones v. Tsige*, 2012 ONCA 32.
[34] *Ibid* at para 70.

> that a reasonable person would regard the invasion as highly offensive *causing distress, humiliation or anguish*. However, proof of harm to a recognized economic interest is not an element of the cause of action. I return below to the question of damages, but state here that I believe it important to emphasize that given the intangible nature of the interest protected, damages for intrusion upon seclusion will ordinarily be measured by a modest conventional sum.[35]

It is also noteworthy that the tort of intrusion upon seclusion is actionable without economic harm. However, the court indicated that an upper ceiling of C$20,000 is appropriate in cases where there is no evidence of economic harm. Punitive and aggravated damages may also be possible in egregious circumstances. The court listed the following factors in relation to assessing damages:

- the nature, incidence and occasion of the defendant's wrongful act;
- the effect of the wrong on the plaintiff's health, welfare, social, business or financial position;
- any relationship, whether domestic or otherwise, between the parties;
- any distress, annoyance or embarrassment suffered by the plaintiff arising from the wrong; and
- the conduct of the parties, both before and after the wrong, including any apology or offer of amends made by the defendant.[36]

1.1.2.3 Scope of Intrusion Upon Seclusion in Ontario

Recently, the tort of intrusion upon seclusion has expanded into the health care sector. In *Hopkins v Kay*,[37] patients from the Peterborough Regional Health Centre (the "Hospital") launched class action lawsuit against the Hospital alleging that approximately 280 patient records were intentionally and unlawfully accessed and disseminated to third parties without the patients' consent.

In response, the Hospital brought a motion to strike the plaintiffs' claim on the basis that it did not disclose a cause of action. The Hospital argued that the claim was precluded by the Ontario *PHIPA* because the legislature intended *PHIPA* to be a comprehensive code that displaces any common law cause of action, including intrusion upon seclusion. Effectively, the Hospital maintained that a plaintiffs' only recourse is to bring a complaint to the Privacy Commissioner.

The Superior Court of Justice dismissed the Hospital's motion to strike, concluding that it was not plain and obvious that the claim disclosed no reasonable cause of action. On December 15, 2014 the Ontario Court of Appeal heard arguments in the appeal of Superior Court's decision. At

[35] *Ibid* at para 71.
[36] *Ibid* at paras. 81-82.
[37] *Hopkins v Kay*, 2014 ONSC 321.

issue was whether the Ontario Superior Court has jurisdiction over *PHIPA* and whether it precludes a private right of action for the tort of intrusion upon seclusion. [38]

The Ontario Court of Appeal released its decision in *Hopkins v Kay* on February 18, 2015.[39] It held that *PHIPA* does not preclude the existence of the common law tort of intrusion upon seclusion, because *PHIPA* does not expressly or impliedly state that it is a comprehensive code that ousts the jurisdiction of the Ontario Superior Court in specific regard to such tort. This was held on the basis of the Court of Appeal's findings that: (a) *PHIPA* expressly contemplates other proceedings in relation to personal health information; (b) *PHIPA*'s review procedure does not ensure that individuals who complain about their privacy in personal health information will have effective redress; and (c) given the nature of the elements of the common law tort, pursuing the common law claim does not conflict with or undermine the scheme established by *PHIPA.*[40]

The tort's reach has also been attempted to be expanded in the cases of *Evans v. The Bank of Nova Scotia*[41] and *Condon v. Canada*[42], which are notable respectively as, the first class action to be certified in Ontario based on the tort of "intrusion upon seclusion" and the largest class action involving a digital privacy breach in Canada.

1.1.2.4 Scope of Intrusion Upon Seclusion Outside Ontario

Recently, the Nova Scotia Supreme Court in *Trout Point Lodge Ltd. v. Handshoe* ("*Handshoe*"), applied the tort of intrusion upon seclusion, as developed in the case of *Jones*, to a case of defamation and invasion of privacy.[43] In *Handshoe*, the plaintiffs brought an action based in defamation, invasion of privacy, and several other torts, against the defendant blogger, who posted many harmful and untrue statements, as well as doctored photographs of the plaintiffs, on his blog. Hood J. considered whether the tort of inclusion upon seclusion, as defined in *Jones*, applied to this case, but she declined to award damages to the plaintiffs under the tort. Hood J. declined to do so because the issue of balancing rights of freedom of expression against privacy rights were not argued. However, she left the door open to the possibility that the tort of intrusion upon seclusion could apply in future cases to award damages to parties whose privacy interests are infringed.[44]

In contrast, intrusion upon seclusion has not been recognized in the province of British Columbia, as enunciated in the recent case of *Demcak v Vo.*[45] In this case, the plaintiffs were subtenants of a rental unit, which was subsequently inspected by the City of Richmond, after the plaintiffs failed to comply with a written notice issued by the city to remove their recreational vehicles from the premises. The plaintiffs were later evicted from the premises by the head tenant for this failure. Subsequently, the plaintiffs, in their statement of claim, alleged that the

[38] *Ibid* at paras. 20-23
[39] 2015 ONCA 112.
[40] *Ibid* at paras. 44-45, 52, 60-62.
[41] 2014 ONSC 2135 (CanLII).
[42] 2014 FC 250 (CanLII).
[43] 2012 CarswellNS 585, 2012 NSSC 245 (NS SC), at paras. 62-65.
[44] *Ibid* at paras. 77-80.
[45] 2013 CarswellBC 1499, 2013 BCSC 899, at para. 8 ["*Vo*"]. See also: *Hung v. Gardiner*, 2002 BCSC 1234 (BC SC) at para. 110 aff'd 2003 BCCA 257 (BC CA) and *Bracken v. Vancouver Police Board*, 2006 BCSC 189 (BC SC) at para. 28.

city committed the common law tort of invasion of privacy. The court held that in British Columbia, section 1 of the provincial *Privacy Act* establishes a statutory tort for invasion of privacy, and therefore it precludes the existence of a common law tort for same.[46] It also held that the city had lawful authorization to enter and inspect the plaintiffs' property and was therefore exempt from the scope of the statutory tort as defined in section 1. As a result, the plaintiffs could not maintain an action for invasion of privacy against the city, and all their claims related to this tort (as well as all others) were dismissed.[47]

1.2 What type of information (including pictures, sounds, etc.) would be covered by the concept of "privacy rights" in the legal system of your country?

While there are variations in the definitions of personal information across the different statutes, the definitions are generally sufficiently broad to encompass pictures and sounds. For example, *PIPEDA* defines personal information as "information about an identifiable individual".[48]

In Ontario, if the information qualifies as "personal health information" such that it includes information about mental or physical health or both, including genetic information, it will likely fall under the scope of Ontario's *PHIPA*.[49] *PHIPA* does not automatically apply to all personal health information. Rather it applies to personal health information that is collected, used and disclosed by health information custodians. All recorded information about an individual that does not fall under personal health information as defined in *PHIPA*, and that is in the custody or under the control of a hospital, is subject to *FIPPA*. However, while personal health information in the custody or control of a hospital is generally governed by *PHIPA*, sections 8, 43(1)(f) and 52(1)(f) of *PHIPA* specify that certain provisions in *FIPPA* also apply.[50]

Ontario's *FIPPA* and *MFIPPA* define "personal information" in the context of privacy rights as:

> … recorded information about an identifiable individual, including,
>
> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
>
> (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
>
> (c) any identifying number, symbol or other particular assigned to the individual,
>
> (d) the address, telephone number, fingerprints or blood type of the individual,

---

[46] *Vo, supra* note 45 at paras. 9-12.
[47] *Ibid* at 12.
[48] *Supra* note 2, s 2(1).
[49] *Supra* note 16 at s. 4(1).
[50] *Applying PHIPA and FIPPA to Personal Health Information: Guidance for Hospitals* (February 2011) Online: Information and Privacy Commissioner of Ontario <https://www.ipc.on.ca/images/Resources/Hospital_guide_Eng.pdf >

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.[51]

The judicial definition of the tort of intrusion upon seclusion, mentioned above, is broad enough to cover a wide range of information, including pictures and sound.

1.2.1 Would the information included in that concept or the extent of the privacy rights depend upon the celebrity of the person or upon other elements? Please describe briefly.

To date, we are unaware of any cases that have taken into consideration the celebrity of an individual as having an impact upon the extent of the individual's privacy rights under *PIPEDA.*

However, it may be worthwhile noting that Section 4(2)(c) of *PIPEDA* exempts an organization from its obligations with respect to personal information where the collecting, using or disclosing is for journalistic, artistic or literary purposes and where the organization does not collect, use or disclose for any other purpose.

In *PIPEDA Case Summary #123*, the Privacy Commissioner considered a complaint by an individual that a local radio station had improperly collected and disclosed his personal information when he called to report a crime he had witnessed.[52] The radio station was a "news-tip" line that listeners may call if they have witnessed a newsworthy event. Callers to the line were often taped, and their interviews used on air. The station tape-recorded the complainant's statement and subsequently used a portion of this recording, along with his name, in a news broadcast. The Privacy Commissioner found that the station was excluded from *PIPEDA* obligations with respect to personal information by s. 4(2)(c). The Commissioner was satisfied that the personal information was collected and disclosed "for journalistic purposes only."

Though not identical to privacy rights, celebrities may have greater recourse at common law under the tort of appropriation of personality. This tort provides protection to an individual seeking (1) to control the use of his or her persona (including personality, image and name) and (2) to prevent others from commercially exploiting his or her personality without consent.[53]

[51] *Supra* note 24, at s 2(1). See also: *Supra* note 25, at s 2(1).
[52] 2003 CarswellNat 5834.
[53] *Krouse v Chrysler Canada Ltd.* (1973), 1 O.R. (2d) 225 (CA).

1.2.2 Would privacy rights apply in relation to legal persons?

Information about a company is generally not personal information for the purposes of *PIPEDA*.[54] However, an individual's personal information may be so inextricably linked to information about his or her company's corporate information such that information about that company can constitute personal information about the individual. This may arise in cases where an individual has both personal and corporate bank accounts at the same bank, and the corporate bank account information kept on file includes detailed information about the individual, such as personal assets. In this case, the corporate information may constitute "personal information" under section 2(1) of *PIPEDA*, depending on its nature.[55] Ultimately, the question of whether corporate information constitutes personal information will need to be assessed on a case-by-case basis.

In addition, the constitutional right to freedom of expression and the right to say nothing has been extended to legal persons such as corporations.[56]

With respect to common law privacy rights such as the Ontario tort of intrusion upon seclusion, it is unlikely that a corporation would be able to make out the required elements. For example, one of the elements that must be demonstrated is that "a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish."[57] It is unlikely that this could apply to a corporation.

1.2.3 Would privacy rights encompass private information made available only to some chosen persons (authorized recipients)? So, for instance, can disclosure to third parties, by one of the authorized recipients of the private information, be part of the privacy rights (e.g. disclosure of private correspondence, private phone calls, information shared on social media, etc.)

1.2.3.1 Application of PIPEDA to Private Communications

PIPEDA does not encompass personal information disclosed between private individuals. Under section 4(1) of *PIPEDA*, the obligations with respect to personal information apply only to: (a) an organization that collects, uses or discloses personal information in the course of commercial activities; or (b) where the personal information is about an employee of the organization and the organization collects, uses or discloses that information in connection with the operation of a federal work, undertaking or business. Section 4(2)(b) of *PIPEDA* excludes from its scope: "any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose."

---

[54] Office of the Privacy Commissioner of Canada, "Legal information related to PIPEDA: Interpretation Bulletin" Online: <https://www.priv.gc.ca/leg_c/interpretations_02_e.asp>.
[55] Office of the Privacy Commissioner of Canada, *Findings under the Personal Information Protection and Electronic Documents Act*(PIPEDA), PIPEDA Case Summary #2003-181, (January 4, 2004), <https://www.priv.gc.ca/cf-dc/2003/cf-dc_030710_05_e.asp>.
[56] *Supra* note 28.
[57] *Jones, supra* note 33 at para. 71.

Despite the fact that *PIPEDA* does not apply to communications between private individuals, the *Criminal Code*[58] makes it a criminal offence to "wilfully [intercept] a private communication."[59] However, s. 148(2) provides a host of exceptions to this offence, such as subsection (a), which provides an exception where one of the parties to the private communication consents to the interception of that communication.

1.2.3.2 Application of Intrusion Upon Seclusion to Private Communications

The tort of intrusion upon seclusion, discussed above, is available to compensate plaintiffs for interceptions of their private communications. In *Jones,* Sharpe J.A. expressly contemplated that intrusion into one's private correspondence would come within the ambit of the tort. Furthermore, in *Ludmer v Ludmer*,[60] the husband respondent, involved in a matrimonial dispute, claimed that a neighbour had hacked into his email account, read his emails, and had forwarded them to the applicant wife's lawyers. The Court accepted that the emails were the respondent's private affairs and thus protected by the tort, but ultimately dismissed the claim for want of evidence.[61] As the Court in *Jones* made clear, however, not all intrusions are actionable. An actionable intrusion into an individual's private communications is one that can be described as highly offensive when viewed objectively by a reasonable person.[62]

1.3 Is there a specific status for "fictional use" of information related to an individual? And are disclaimers sufficient to allow such use?

In *Citi Cards Canada Inc. v Pleasance*, the Ontario Court of Appeal noted that the definition of personal information in *PIPEDA* is "elastic" and "should be interpreted in that fashion to give effect to the purpose of the Act"[63] Similarly, in *Dagg v Canada (Minister of Finance)*, the Supreme Court of Canada, in interpreting the definition in the federal *Privacy Act*, commented that, "on a plain reading, this definition is undeniably expansive."[64]

PIEPDA does not distinguish between factual and fictional information. Presumably, therefore, if information is "about" an "identifiable" "individual", it is "personal information" under *PIPEDA*. The key element of the definition is identifiability – i.e. can the information be attributed to a specific individual? Thus, the information itself does not necessarily have to identify an individual. It will constitute "personal information" if it is reasonably capable of identifying an individual. If a person could combine the information in question with information from other sources, the individual is identifiable. In Ontario, it has been held that if there is a "reasonable expectation" that an individual can be identified from information, then such information qualifies as personal information.[65]

With respect to a specific status in Canadian law for the use of actual personal information that is presented as thinly veiled fiction or used for artistic purposes, which later causes harm to the

[58] RSC, 1985, c C-46.
[59] *Ibid* at s. 148(1).
[60] 2013 ONSC 784
[61] *Ibid* at paras 290-314, aff'd 2014 ONCA 827, at paras 47-50.
[62] *Jones, supra* note 33 at paras. 71-72.
[63] 2011 ONCA 3, at para 22.
[64] 1997, 148 DLR (4th) 385, at para 68.
[65] *Ontario (Attorney General) v Pascoe*, 110 ACWS (3d) 585 (Ont Div Ct), at para 14.

individual, remedies may be available under the tort of appropriation of personality, as discussed above.

We are not aware of any cases which address the effectiveness of disclaimers in relation to fictional use.

2 Freedom of Speech

2.1 Is there a statutory/treaty-based freedom or constitutional recognition of freedom of speech or is that freedom based on case-law?

2.1.1 Constitutional Recognition

Freedom of thought and expression is constitutionally recognized. Section 2 of the *Charter* states:

> Everyone has the following fundamental freedoms:
> (*a*) freedom of conscience and religion;
> (*b*) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;
> (*c*) freedom of peaceful assembly; and
> (*d*) freedom of association.[66]

2.1.2 Scope of Freedom of Expression

2.1.2.1 R v Keegstra

The leading case on the scope of freedom of expression in section 2(b) of the *Charter* is *R v Keegstra ("Keegstra").*[67] The issue in this case was whether a section in the *Criminal Code*, making it an offence to wilfully promote hatred against an identifiable person or group, infringed Mr. Keegstra's right to freedom of expression when he disseminated hate propaganda. On this issue it was held that even hate propaganda is protected under section 2(b) of the *Charter*: "if the activity conveys or attempts to convey a meaning, it has expressive content and *prima facie* falls within the scope of the guarantee" under section 2(b).[68] Despite this finding, the court ultimately found that Mr. Keegstra's right to freedom of expression was justifiably infringed under section 1 of the *Charter*, and therefore the criminal code section at issue was upheld as constitutional. The important point to take away from *Keegstra* is that freedom of expression under section 2(b) is not an absolute right, and is subject to a balance with other competing societal values and objectives.[69]

---

[66] Supra note 26.
[67] 1990 CarswellAlta 192, [1990] 3 S.C.R. 697 (S.C.C.).
[68] *Ibid* at 34.
[69] *Ibid* at 77. See also *Saskatchewan (Human Rights Commission) v. Whatcott*, 2013 SCC 11, at paras. 6, 66, ["*Whatcott*"].

2.1.2.2 Other Cases

Section 2(b) of the *Charter* has been interpreted by courts to protect "postering, commercial expression, access to government information, and all manner of political protests. Freedom of expression implies freedom to refrain from expression."[70]

"Subsection 2(b) protects all forms of expression that are capable of meaning other than expression through physical violence."[71] Human rights legislation limiting freedom of expression has been found to be constitutional where the expression exposes "a protected group to hatred or contempt" and goes "beyond that which ridicules, belittles, or otherwise affronts the dignity of the group."[72]

Cases subsequent to *Keegstra* have affirmed that freedom of expression, although recognized as an important *Charter* right, is not absolute in Canada. For example, in *Saskatchewan (Human Rights Commission) v Whatcott*,[73] the Supreme Court upheld the hate speech provisions of the Saskatchewan *Human Rights Code*, which prohibit any representation that "exposes or tends to expose to hatred, ridicules, belittles or otherwise affronts the dignity of any person or class of persons on the basis of a prohibited ground."[74] The appellant, Mr. Whatcott, was fined $17,500 by the Saskatchewan Human Rights Commission for distributing anti-homosexual flyers. The Supreme Court found that while the hate speech provisions infringed Mr. Whatcott's freedom of expression guaranteed under s. 2(b) of the *Charter*, the infringement was justified under s. 1. Significantly, the Court found that only a prohibition on speech that rises to the level of "hatred" was constitutionally valid. Other language in the *Human Rights Code* prohibiting speech that "ridicules, belittles, or otherwise affronts the dignity" of an individual, was not justified under s. 1 because, unlike "hatred", it was aimed at something less than harmful expression. As part of its s. 1 balancing exercise, the Court also considered that hate speech does little to promote the values underlying freedom of expression and that it can distort or limit the free exchange of ideas by its tendency to silence the voice of its target group.

2.2 If it is a statutory/treaty/constitution based freedom is it based on domestic or supranational law?

The constitutional right to freedom of expression is domestic law. However, the freedoms protected by s 2(b) of the *Charter* "are recognized in international treatises as being essential to human dignity."[75]

---

[70] The Law Society of Upper Canada, *Licensing Process Study Materials 2014: Barrister* (Toronto: The Law Society of Upper Canada, 2014) at 579.
[71] *Ibid*.
[72] *Ibid* at 579-580.
[73] *Whatcott*, *supra* note 69.
[74] *Ibid* at 12.
[75] *Supra* note 70 at 579.

2.3 Describe the main characteristics of freedom of speech as recognized in your jurisdiction: (a) beneficiaries; (b) extent of the freedom of speech; (c) exceptions; and (d) specific status for press (including online press).

Freedom of expression applies to "everyone." This right benefits "individuals (citizens and non-citizens) as well as corporations."[76]

Freedom of expression can be limited by s 1 of the *Charter*, which reads as follows:

> The *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.[77]

"While the burden of establishing an infringement of the *Charter* rests with the party alleging it, the onus of proving that the infringement is reasonably and demonstrably justified in a free and democratic society rests upon the party seeking to uphold the limitation on a balance of probabilities."[78] In *R v Oakes*,[79] the Supreme Court of Canada established a test for determining whether a limitation on a right such as freedom of expression is reasonably and demonstrably justified in a free and democratic society under s 1 of the *Charter*:

> Two requirements must be satisfied to establish that a limit is reasonable and demonstrably justified in a free and democratic society. First the legislative objective which the limitation is designed to promote must be of sufficient importance to warrant overriding a constitutional right. It must bear on a "pressing and substantial concern." Second, the means chosen to attain those objectives must be proportional or appropriate to the ends. The proportionality requirement, in turn, normally has three aspects: the limiting measures must be carefully designed, or rationally connected, to the objective; they must impair the right as little as possible; and their effects must not so severely trench on individual or group rights that the legislative objective, albeit important, is nevertheless outweighed by the abridgment of rights.[80]

There are numerous examples of courts using section 1 of the *Charter* to limit freedom of expression. For example, courts have used section 1 to uphold laws prohibiting election advertising on polling days[81] and injunctions against picketing.[82]

The press, either online or otherwise, is not afforded special status under the constitution. However, many constitutional challenges citing freedom of expression have been brought by newspaper chains.

---

[76] *Ibid* at 579-580.
[77] *Supra* note 26.
[78] *Supra* note 70 at 582.
[79] [1986] 1 S.C.R. 103, [1986] S.C.J. No. 7 (SCC), ["Oakes"].
[80] *Ibid* at paras. 73-75.
[81] *Supra* note 28, citing *Harper v Can.* [2004]1 SCR 827.
[82] *Ibid*, citing *BCGEU v B.C. (Vancouver Courthouse)* [1988] 2 SCR 214.

3 Hierarchy Between Freedom of Speech and Privacy Rights

3.1 Under the law applicable in your jurisdiction, is there a clear hierarchy between freedom of speech on the one hand and privacy rights on the other?

There is no clear hierarchy between freedom of expression and privacy rights. In cases where new laws pit privacy rights against freedom expression, courts would approach such situations on a case-by-case basis and make decisions based on the merits of each case.

For example, in *United Food*[83], the Supreme Court of Canada considered whether Alberta's *PIPA* unjustifiably limited a union's right to freedom of expression in the context of a lawful strike. The union recorded and photographed individuals crossing its picket line for use in its labour dispute. Several individuals complained to the privacy commissioner. The union argued, successfully, that *PIPA* infringed its right to freedom of expression under s. 2(b) of the *Charter*.

The Court in *United Foods* determined that the infringement of the respondent union's section 2(b) right was not justified, as required by s. 1 of the *Charter*. The traditional test from *R v Oakes* was applied.[84] The onus was on the government to show that the impugned legislation had (1) a pressing and substantial objective, and (2) that the means employed were reasonable and demonstrably justified. In the latter regard, the government had to show that the means were (i) rationally connected to the objective, (ii) minimally impairing of the right or freedom in question, and (iii) proportionate to the objective.

Applying this test, the Court determined that *PIPA* had a pressing and substantial objective – providing an individual with some measure of control over his or her personal information. Information privacy, the Court noted, plays an important role in preserving a free and democratic society.[85] Furthermore, providing an individual with control over his or her personal information is also "intimately connected" to "significant social values" such as individual autonomy and dignity.[86]

The Court then determined that while the provisions of *PIPA* limiting the union's freedom of expression were rationally connected to their objective, they were disproportionate to the benefits of the legislation. *PIPA* did not provide any way to accommodate the expressive purposes of unions engaged in lawful strikes. It provided a general prohibition against the union's use of personal information (absent consent or deemed consent) to further its collective bargaining objectives, without any balancing of the union's constitutional right to freedom of expression. Specifically, the personal information collected, used and disclosed by the union was taken from an open political demonstration and was limited to images of individuals crossing a picket line. The information did not include individuals' intimate biographical details.[87] *PIPA*'s deleterious effects stemmed from the prohibition noted above, which impeded the union's expressive purposes. These purposes included: ensuring the safety of union members, attempting to persuade the public not to do business with an employer, and bringing the debate on labour

[83] *United Food, supra* note 20.
[84] *Oakes, supra* note 79.
[85] *United Food, supra* note 20, at para. 19.
[86] *Ibid* at para. 24.
[87] *Ibid* at para. 26.

conditions into the public realm. Moreover, the specific act of picketing is a particularly crucial form of expression in the labour relations context.

The Court concluded as follows: "…like privacy, freedom of expression is not an absolute value and both the nature of the privacy interests implicated and the nature of the expression must be considered in striking an appropriate balance."[88]

3.2 What would be the most significant criteria allowing freedom of speech or privacy rights to prevail over the other (e.g. public interest argument)?

Please see the previous discussion under section 3.1. The *United Food* case provides a topical example of the balancing that courts in Canada perform when weighing freedom of speech and privacy rights. The test in *R v Oakes* is applied in all *Charter* cases.

4 Remedies to Protect Against Disclosure of Personal Information

4.1 Are there pre-emptive remedies to avoid disclosure of such information before disclosure occurs? Describe briefly the main remedies available.

Injunctions are generally available in most Canadian jurisdictions, which can be sought from a court to prevent the release of private information. In order to be entitled to an injunction, the parties must satisfy the three branches of the test established by the Supreme Court of Canada in *RJR-Macdonald Inc. v. Canada*:[89]

> (a) Is there a serious issue to be tried?
>
> (b) Will the applicant suffer irreparable harm if the injunction is not granted?
>
> (c) Which party will suffer the greatest harm from granting or refusing the injunction, i.e. where does the balance of convenience lie?[90]

4.2 Are "gagging orders" or "super injunctions" as known in the UK known under the legal system of your country? Describe briefly their main characteristics.

Super injunctions, as they are known in the United Kingdom, prohibit the parties from disclosing the existence of the injunctions granted to supress disclosure of personal information. They appear to be rarely granted by courts in the United Kingdom, and are granted to protect the privacy of public figures and celebrities, whose personal information would have otherwise been disclosed.[91] Super-injunctions are not currently part of Canadian law.[92] Canadian authorities offer

[88] *Ibid* at para. 38.
[89] [1995] 3 S.C.R. 199 (S.C.C.).
[90] *Ibid* at 49-67.
[91] Ryder Gilliland and Erin Hoult, "Super Injunctions: Enforcing gag orders in the Internet age", (March 6, 2012), <http://www.lawyersweekly.ca/index.php?section=article&articleid=1129>.
[92] *Ibid.*

support for the view that super-injunctions are simply incompatible with the principle of the openness of the judicial system.[93]

In *Injunctions and Specific Performance*, Robert J. Sharpe criticizes super-injunctions as belonging to the domain of "secret justice" incompatible with the open court principle that enjoys a prominent place in the Canadian legal system:

> "Super-injunctions" pose the spectre of secret justice that undermines the open court principle and the rights of third parties who are bound by orders of which they had no prior notice. "Super-injunctions" have also proved difficult to enforce in the era of social media. It is submitted that as the right to privacy does not enjoy the same pre-eminence under the Charter, there is no place for "super-injunctions" in Canadian law.[94]

Public interest immunity, a concept recognized in Canada, has some overlap with U.K. super-injunctions, in the sense that both may aim to prevent the disclosure of personal or private information of individuals in court proceedings and in the media. However, these two concepts have significantly different objectives. Moreover, public interest immunity is a remedy available only to government officials. According to the *Canadian Encyclopedic Digest*:

> Both the common law and the *Canada Evidence Act* recognize public interest immunity as a right of the government to object to the production or admissibility of otherwise relevant information on the grounds of public interest. Successful claims of immunity demonstrate that the public interest in maintaining confidentiality outweighs the interest in allowing the tribunal to have access to the relevant information to ensure the proper administration of justice.
>
> To assess the public interest in disclosure, the judge should consider factors such as: the importance of the litigation; the necessity of the evidence for the correct determination of disputed facts; whether the issues concern an allegation of governmental misconduct; and the overall need for fairness in the hearing. Where the immunity is claimed during a criminal trial, the court must also consider whether upholding the claim would prevent the defendant from making full answer and defence to the charges. In these circumstances, the court may consider upholding the privilege and dismissing counts in the information or staying the proceedings altogether.[95]

---

[93] *Ibid.* See also *R v Eurocopter*, 2003 CanLII 32308 (ON SC), where the Ontario Superior Court undertook an extensive review of Canadian jurisprudence with respect to the relationship between individual privacy and the principle of open courts and *A.G. of Nova Scotia v MacIntyre* (1982), 65 CCC 129 (SCC), per Dickson J.
[94] *Ibid* citing Robert J. Sharpe, Injunctions and Specific Performance, loose-leaf (consulted on March 6, 2012), (Toronto, Ont: Canada Law Book, 2012), Ch 5 at 5.185.
[95] *CED* Evidence XV.8.(b).(i), Evidence | XV — Privilege | 8 — Public Interest Immunity | (b) — Information in the Public Interest | (i) — Balancing Test.

4.3 Are there other post-disclosure remedies, such as damage claims, rectification claims or right of answer?

4.3.1 Damages

Courts may award damages under both the tort of intrusion upon seclusion,[96] and under *PIPEDA*. With respect to *PIPEDA*, section 16(c) of the statute gives the court the discretion to award damages to the complainant, including damages for any humiliation that the complainant has suffered.[97]

4.3.2 Investigation

Section 12 of *PIPEDA* provides two avenues for the initiation of an investigation where an individual's personal information has been collected, used, or disclosed in contravention of *PIPEDA*. The first avenue for a possible investigation is if an individual files a written complaint with the Commissioner in respect of an organization's alleged violation.[98] The second avenue for possible investigation grants the Commissioner discretion to initiate a complaint on an individual's behalf, if the Commissioner is satisfied that there are reasonable grounds to investigate a matter.[99]

Pursuant to section 12(1) of *PIPEDA*, the Commissioner shall conduct an investigation in respect of a complaint, unless the Commissioner is of the opinion that:

> (*a*) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;
>
> (*b*) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province; or
>
> (*c*) the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose.[100]

4.3.3 Powers of Commissioner Conducting Investigation

If the Commissioner proceeds with an investigation, he or she can employ any or all of the following measures as part of the investigation of a complaint:

> (*a*) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;

---

[96] *Jones*, *supra* note 33.
[97] *Supra* note 2.
[98] *Ibid* at s. 11(1).
[99] *Ibid* at s. 11(2).
[100] *Ibid* at s. 12(1).

(*b*) administer oaths;

(*c*) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;

(*d*) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises;

(*e*) converse in private with any person in any premises entered under paragraph (*d*) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and

(*f*) examine or obtain copies of or extracts from records found in any premises entered under paragraph (*d*) that contain any matter relevant to the investigation.[101]

As part of an investigation, the Commissioner may attempt to employ dispute resolution mechanisms such as mediation or conciliation to resolve a particular complaint.[102]

4.3.4 Commissioner's Report

Within one year after the day on which an individual files a written complaint or the complaint is initiated by the Commissioner, the Commissioner must prepare a report which contains findings and recommendations and any settlement that was reached by the parties. If appropriate, the report should also include a request that the organization give the Commissioner, within a specified time, notice of any proposed or actual action it has taken to comply with recommendations set out in the report. Furthermore, the report should set out any recourse that the complainant could pursue in court.[103]

4.3.5 Application for Court Hearing

After an individual complainant receives the Commissioner's report, the individual can apply for a court hearing on the matter. As part of the hearing, the court has wide discretion to grant remedies to the complainant, including the power to:

(a) order an organization to correct its practices in order to comply with *PIPEDA*;

(b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and

(c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.[104]

---

[101] *Ibid* at s. 12.1(1).
[102] *Ibid* at s. 12.1(2).
[103] *Ibid* at s. 13(1).
[104] *Ibid* at s. 16.

4.3.6 Commissioner's Audit Powers

Pursuant to section 18(1) of *PIPEDA*, the Commissioner has the power, at any time, after providing an organization with reasonable notice, to audit its personal information management practices, if the Commissioner has reasonable grounds to believe that the organization is contravening *PIPEDA*. As part of an audit, the Commissioner has wide powers including the ability to summons persons to give written or oral evidence or order them to produce any relevant records, enter the physical premises of any organization to examine or obtain copies of relevant records, and accept and receive any evidence regardless of whether or not it is admissible in a court of law.

After an audit is completed, the Commissioner must provide the audited organization with a report which contains the findings of the audit and any recommendations that the Commissioner considers appropriate.[105]

4.3.7 Rectification

As noted earlier, *PIPEDA* requires compliance with certain principles set out in Schedule 1 thereof. The principle of individual access provides that upon request, an individual must be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. It also provides that an individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.[106] This principle provides an express right of rectification.

4.3.8 Right of Answer

In the province of Quebec, the *Quebec Press Act* ("*QPA*") gives any person who claims to have been injured by any article published in a newspaper or periodical the "right of answer" or right to reply to that article.[107] Specifically, the *QPA* provides that the newspaper or periodical must publish, at its own expense, any written reply to any article by any individual alleged to have been injured by it.[108]

The right of answer featured in the *QPA* also exists in a slightly different form in Ontario, called a "right of retraction", however it is not a right that entitles a harmed individual to a right of answer. Rather, the *Libel and Slander Act*[109] provides that where an individual alleges libel or slander and files a written complaint with a newspaper or broadcaster, the newspaper or broadcaster has the discretion to publish a "full and fair retraction" of their earlier article to limit their liability to actual provable damages.[110] In a sense, this provides a partial remedy to an individual actually harmed by a defamatory article or spoken statement.

---

[105] *Ibid* at s. 19(1).
[106] *Ibid* at Schedule 1, s 4.9.
[107] c. P-19.
[108] *Ibid* at s. 7.
[109] R.S.O. 1990, c L.12
[110] *Ibid* at s. 5(1) - 5(2).

4.4 In the case of damages, how are they calculated?

4.4.1 Common Law

Under the common law tort of intrusion upon seclusion, the following factors are frequently considered by courts, and provide a useful guide in assessing the appropriate quantum of damages:

- the nature, incidence and occasion of the defendant's wrongful act;
- the effect of the wrong on the plaintiff's health, welfare, social, business or financial position;
- any relationship, whether domestic or otherwise, between the parties;
- any distress, annoyance or embarrassment suffered by the plaintiff arising from the wrong; and
- the conduct of the parties, both before and after the wrong, including any apology or offer of amends made by the defendant.[111]

If there is pecuniary loss, the courts will award damages accordingly. Without pecuniary loss, the damages are likely to be at or under C$20,000. The court in *Jones* stated they would not exclude awards of aggravated and punitive damages in exceptional cases calling for exceptional remedies. However, the court went on to state that they would not encourage such awards (absent exceptional circumstances) as predictability and consistency in award damages are paramount values in an area where symbolic or moral damages are awarded.[112]

4.4.2 PIPEDA

Under the statutory regime set out in *PIPEDA*, Zinn J. of the Federal Court of Canada in *Nammo v TransUnion of Canada Inc.* applied the same approach the Supreme Court of Canada uses in determining damages in *Charter* cases to determine damages under s 16(c) of PIPEDA[113]:

> …The Supreme Court addressed the different goals of awarding damages for a *Charter* breach; these include compensation, for which loss is relevant, but also vindication and deterrence, for which loss is not a determinative factor. … [114]

The Supreme Court found that "to be 'appropriate and just', an award of damages must represent a meaningful response to the seriousness of the breach and the objectives of compensation, upholding *Charter* values, and deterring future breaches." It appears that the same reasoning applies to a breach of *PIPEDA*.[115]

---

[111] *Jones, supra* note 33, at paras. 81-82, 87.
[112] *Ibid* at paras. 87-88.
[113] *Nammo v. TransUnion of Canada Inc*., 2010 FC 1284 (CanLII), <http://canlii.ca/t/2f3lz>.
[114] *Ibid* at paras. 72-73, 77.
[115] *Ibid* at para. 74.

As discussed above in section 1.1, the federal Commissioner under PIPEDA does not have order-making powers. Therefore, the Commissioner cannot award damages to an injured complainant if it is found that an organization breached an obligation to the complainant under PIPEDA. However, if the matter is heard by the Federal Court of Canada, after the Commissioner has released a report on its investigation, the court may award damages to the complainant under section 16(c) of PIPEDA.

4.5 In case of unauthorized disclosure of private information, who can be held liable for damages, especially online?

In general, the party found to have breached its obligations under *PIPEDA* or the party found to have committed the tort of intrusion upon seclusion would be held liable for damages.

4.5.1 Liability of Intermediaries

The Supreme Court of Canada case of *Crookes v Newtown* ("Crookes")**,** while not dealing directly with privacy issues, developed important principles regarding acts which do and do not constitute the *publication* of defamatory material on the internet.[116] In this case, the issue was whether the creation of a hyperlink to allegedly defamatory material constitutes publication of that material. The Supreme Court held that a hyperlink, on its own, does not constitute publication of the allegedly defamatory content to which it refers.[117] Furthermore, publication of defamatory content will only occur in this context if the hyperlink also contains and repeats defamatory content directly onto the same website where the hyperlink is located.[118]

In the Supreme Court's reasoning, Abella J. referenced case law from the United Kingdom in which internet service providers and search engine operators were not held liable as publishers of defamatory content, because they only acted as intermediaries and acted without any knowledge that the content being published was actually defamatory. The guiding principle in these cases is that where an internet service provider acts in an extremely passive manner, it is unlikely they will be held liable for defamation.[119]

4.5.2 Application of *Crookes* to Privacy Breaches

The principle above could apply equally to privacy laws and specifically *PIPEDA*. However this has not been established in Canadian jurisprudence. For example, where an internet service provider hosts or transmits personal information of an individual without their consent, but the service provider does not have actual knowledge or a reasonable basis to suspect that the information has been posted and disclosed online by a third party without that individual's consent, it is unlikely that the service provider will be found to be in breach of section 7(3) or Schedule 1 of *PIPEDA*.

However, the reasoning from Abella J. could also apply to find internet service providers in breach of section 7(3) of *PIPEDA*. This could occur in circumstances where individuals have

[116] 2011 SCC 47, 3 S.C.R. 269, ["*Crookes"*].
[117] *Ibid* at 14.
[118] *Ibid* at 24-27.
[119] *Ibid* at 89-92.

brought it to the attention of internet service providers that their personal information has been posted online by a third party without their consent, and the service providers subsequently refuse to remove that information from their websites. Moreover, service providers may also be found to be in breach of 4.9.5 of Schedule 1 of *PIPEDA* if they have received complaints from individuals who want to rectify inaccuracies in personal information posted online, but then service providers later refuse to correct them. In these circumstances, if individuals subsequently file written complaints with the Privacy Commissioner, they may also choose to proceed with court hearings pursuant to section 14(1). Therefore, it is a possibility that courts may award individuals damages for the harm they have suffered, including humiliation, pursuant to section 16 (c) of *PIPEDA*. It should be noted again that this is a hypothesis, given that it has yet to arise in Canadian jurisprudence. Therefore, it remains to be seen whether *PIPEDA* would apply in this context.

Within the context of defamation law, the recent case of *Weaver v Corcoran*[120] clearly suggests that liability of an otherwise passive intermediary will be impacted by their awareness of defamatory comments posted by others. One of the issues addressed by the court was the extent to which the website of a newspaper would be liable for defamatory comments posted by its readers. On this point, the court concluded as follows:

> Until awareness occurs, whether by internal review or specific complaints that are brought to the attention of the National Post or its columnists, the National Post can be considered to be in a passive instrumental role in the dissemination of the reader postings. It has taken no deliberate action amounting to approval or adoption of the contents of the reader posts. Once the offensive comments were brought to the attention of the defendants, however, if immediate action is not taken to deal with these comments, the defendants would be considered publishers as at that date.[121]

Again, it remains to be seen whether this principle might apply in relation to privacy breaches.

4.6 Are there special defences to a cause of action for information disclosed by the press/media?

While not exactly a defence, section 4(2)(c) of *PIPEDA* indicates that it does not apply to any organization that collects, uses, or discloses personal information solely for journalistic, artistic, or literary purposes.[122] For example, media organizations are not required to: designate individuals who are accountable for their compliance with the *PIPEDA* principles, identify the purposes for which personal information is being collected, used or disclosed, obtain consent from individuals before collecting, using or disclosing their personal information, or implement security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.[123]

---

[120] 2015 BCSC 165.
[121] *Supra* para 284.
[122] *Supra* note 2 at s. 4(2)(c) and 5(1).
[123] *Ibid* at Schedule 1, principles 4.1, 4.2, 4.3, and 4.7.

4.7 Is there any specific case-law in your country relating to social media, and if so please summarize this?

In Canada, *PIPEDA* has had a significant impact on the operations of social media websites. One important example is a recent case from 2012 involving Facebook and its "Friends Suggestion" function.[124] In this case, three complainants received personal email invitations to join Facebook, along with "friend suggestions"- a list of Facebook users that the complainants appeared to know and could "friend" if they decided to join the website. None of the complainants were Facebook users themselves, and therefore they believed that Facebook had inappropriately accessed their email address books (or that of their friends) to generate lists of suggested Facebook friends.

The Privacy Commissioner of Canada investigated this matter and did not find any evidence that Facebook had accessed the email address books of the complainants, or was maintaining personal profiles about non-users. However, the Commissioner found that email addresses were personal information, and that Facebook had failed to meet the knowledge and consent requirements of *PIPEDA*. Specifically, Facebook failed to initially identify the purposes for which their email addresses would be used, prior to collecting them. Facebook also failed to take reasonable measures to ensure that non-users were *made aware* that their email addresses were being collected for the purpose of generating suggested friends. Facebook also failed to obtain the knowledge and consent of non-users prior to using their email addresses to generate friend suggestions.

Facebook subsequently corrected its breaches of *PIPEDA* by providing non-users with clear and adequate notice that it will use their e-mail addresses to generate lists of suggested friends. It also created an "opt-out" mechanism for non-users in the form of an unsubscribe button in their email invitations, such that they could decline to consent to their emails being used to generate suggested lists of Facebook friends. It is interesting to note that the Commissioner stated that in these circumstances, the opt-out mechanism for obtaining consent was appropriate because the use of a non-user's email address to generate social connections seen only by the non-user would not generally be considered sensitive in nature.[125]

4.8 Are there specific remedies against disclosure of information that (could) damage an individual reputation (such as slander or libel)? Describe these remedies briefly.

4.8.1 Defamation (Libel and Slander)

Privacy offences and defamation are separate causes of action. Defamation is unlikely to apply in a case of mere disclosure of private information. Although the elements of defamation could be made out by mere disclosure of private information, the defence of truth is likely to apply (assuming the disclosed information is accurate). Below is a brief statement of defamation law in Canada from the *Canadian Encyclopedic Digest*:

[124] Office of the Privacy Commissioner of Canada, *PIPEDA* Report of Findings #2012-002, <https://www.priv.gc.ca/cf-dc/2012/2012_002_0208_e.asp.>.
[125] *Ibid* at 45-46.

Defamation consists of any written, printed or spoken words or of any audible or visible matters or acts which tend to lower a person in the estimation of others or cause a person to be shunned or avoided or exposed to hatred, contempt or ridicule. Thus an assertion which does not suggest discreditable conduct by the plaintiff may still be defamatory if it imputes to him or her a condition calculated to diminish the respect and confidence in which the plaintiff is held.

A plaintiff in a defamation action is required to prove three things to obtain judgment and an award of damages: (1) that the impugned words were defamatory, in the sense that they would tend to lower the plaintiff's reputation in the eyes of a reasonable person; (2) that the words in fact referred to the plaintiff; and (3) that the words were published, meaning that they were communicated to at least one person other than the plaintiff.[126]

4.8.2 Defences to Defamation

The law of defamation must strike a fair balance between the protection of reputation and the protection of free speech. In turn, a statement is not actionable, despite the fact that it is defamatory, if one of five defences are established:

- Justification: the statement is true
- Absolute privilege: the statement is made in Parliament, made as evidence at a trial, or contained in court documents
- Qualified privilege: this defence is available where remarks that may otherwise be defined as defamatory were conveyed to a third party non-maliciously and for an honest and well-motivated reason.
- Fair comment: Honest statements of opinion, based on fact, are not malicious and are not considered defamatory.
- Responsible communication on matters of public interest: Journalists and news reporters can report statements and allegations (even if they are not true) if there is a public interest in distributing the information to a wide audience.[127]

These defences are of crucial importance in the law of defamation because of the low level of the threshold over which a statement must pass in order to be defamatory.[128]

4.8.3 Common Law Remedies

4.8.3.1 Apology

In the context of publishers and newspapers who print libelous statements that rise to the level of defamation, apologies by the organization which prints them is a form of remedy to the injured

[126] *CED* Defamation I.1, Defamation | I — General | 1 — Defamation Defined, ["*Defamation*"].
[127] *Canadian Encyclopedic Digest*- VII- X.A
[128] *Defamation*, *supra* note 126.

party. The apology may mitigate the organization's damages, depending on their content and timing.[129]

4.8.3.2 Injunctions

In general, courts are reluctant to grant injunctions in defamation actions; they are only granted on rare occasions.[130] Before an interlocutory or interim injunction is granted, a plaintiff must establish that the words are clearly defamatory and untrue[131], such that no defence of justification would succeed,[132] and where applicable must also show that the words are not fair comment on true or admitted facts.[133]

4.8.3.3 Damages

Damages in a libel or slander action may include:

> a) special damages, where an actual monetary loss attributable to the libel is proved, such as the loss of a contract or a job;
>
> b) general damages to compensate for the harm done to the plaintiff's reputation in the community and for humiliation;
>
> c) aggravated damages which are compensatory in nature but are awarded where the defendant's conduct has been particularly high-handed, malicious, or oppressive; and
>
> d) punitive damages, to punish the defendant's conduct;[134]

4.8.4 Statutory Remedies

In all Canadian provinces, legislation governs defamation actions based in libel against newspapers, television broadcasters, and publishers. In Ontario, the *LSA* governs libel actions against these specific media defendants, as well as slander actions brought against any individual or organization (not limited to media defendants).[135] In Ontario, it is still unclear whether the scope of the *LSA* applies to defamation actions with respect to internet publications.[136]

---

[129] See *Allan v Bushnell T.V. Co.* [1969] 2 O.R. 6 (Ont. C.A.); *Munro v Toronto Sun Publishing Corp* (1982), 39 O.R. (2d) 100 (Ont. H.C.J) at para 65; *Tait v New Westminster Radio Ltd*. (1984), 58 B.C.L.R. 194 (B.C. C.A.).
[130] *Canada (Human Rights Commission) v Canadian Liberty Net,* [1996] 1 F.C. 804 at para. 22 (C.A.), aff'd 157 D.L.R. (4th) 385 (S.C.C.).
[131] *Canada (Human Rights Commission) v Canadian Liberty Net*, [1998] 1 S.C.R. 626, at para. 49.
[132] *Canada Metal Co. v Canadian Broadcasting Corp.* (1975), 7 O.R. (2d) 261n (Ont Div. Ct.).
[133] *Pilot Insurance Co. v Jessome*, [1993] O.J. No. 172 (Gen. Div).
[134] Pepper, Morritt, Stephenson, and Ross, *Canadian Defamation Law and Practice*, Release No. 3, (Toronto, ON: Thomson Reuters Canada Limited, November 3, 2014), at 5-14.
[135] *Supra* note 109 at s. 1-15, s. 15-24.
[136] *Shtaif v. Toronto Life Publishing Co. Ltd.*, 2013 ONCA 405. See *Bahlieda v. Santa*, 2003 CanLII 2883 (Ont. C.A.)

4.8.4.1 For Libel

In Ontario, before a plaintiff can recover damages in a libel action against a newspaper or broadcaster, she must, within six weeks after the alleged libel has come to her knowledge, give written notice to the defendant detailing the complaint.[137] In addition to this notice requirement, the plaintiff must also commence a libel action against the relevant newspaper or broadcaster within three months after the alleged libel has to come to her attention.[138] Once these pre-conditions are met, and assuming the plaintiff has satisfied all criteria for an action in defamation and no defences are made out, all remedies available at common law are potentially available. However, section 5(2) of the *LSA* provides that a plaintiff will only be able to recover *actual damages* in a libel action if the defendant satisfies all of the following conditions:

- the alleged defamatory material was published in good faith;
- the material did not impute to the plaintiff the commission of a criminal offence;
- the publication took place in mistake or misapprehension of the facts; and
- the statutory terms regarding retraction were satisfied by the defendant within the required time. [139]

4.8.4.2 For Slander

Pursuant to the *LSA*, in an action for slander involving words calculated to disparage the plaintiff in any office, profession, calling, trade or business held or carried on by the plaintiff at the time of the publication thereof, the plaintiff is not required to allege or prove special damage.[140] In other words, these are actionable *per se*.[141] This also applies with respect to actions for slander of title, slander of goods or other malicious falsehood, if the plaintiff establishes either of the two enumerated criterion in the statute.[142] It appears that all common law remedies mentioned above are also potentially available for these causes of action, with the necessary damages modifications as discussed.

4.9 Forum and Applicable Law

4.9.1 Describe shortly what rules exist in your jurisdiction for the determination of the forum and the applicable law.

According to the Commissioner, *PIPEDA* was not initially intended to apply beyond Canada's borders. However it may apply extra-territorially depending on the circumstances of an individual case.[143] It is also the position of the Commissioner that it has jurisdiction to investigate complaints relating to the trans-border flow of personal information. Furthermore, *PIPEDA* may apply to foreign entities that either receive or transmit communications to and from Canada, or

---

[137] *Supra* note 109 at s. 5(1).
[138] *Ibid* at s. 6.
[139] *Ibid* at s. 5(2). See also: *Ungaro v. Toronto Star Newspapers Ltd.* (1997), 1997 CarswellOnt 232 (Ont. Gen. Div.)
[140] *Ibid* at s. 16.
[141] John G. Fleming, *The Law of Torts*, 9th ed. (1998: LBC).
[142] *Supra* note 109 at s. 17.
[143] Office of the Privacy Commissioner of Canada, *PIPEDA and Your Practice: A Privacy Handbook for Lawyers*, (August 16, 2011), < https://www.priv.gc.ca/information/pub/gd_phl_201106_e.asp#_edn14>.

that collect and disclose personal information about individuals in Canada. Ultimately, however, case law provides that the application of *PIPEDA* to a foreign entity will be determined on a case by case basis depending on whether the foreign entity at issue has a real and substantial connection to Canada.[144]

There is limited case law on the application of *PIPEDA*'s scope to foreign entities carrying on commercial activities beyond Canada's borders which collect, use or disclose personal information of Canadians. However, a 2008 finding from the Commissioner suggests several factors that a court may consider in its determination of whether a foreign entity has a real and substantial connection to Canada, and is therefore subject to *PIPEDA*:

- The foreign entity collects personal information from and disclosed it to Canadian organizations
- The foreign entity charges the Canadian entity fees for its services relating to collection of personal information;
- The citizenship of any shareholders or owners of the foreign entity;
- Whether any officers or directors of the foreign entity are also employed by a Canadian organization;
- Whether the majority of cross-border transfers of personal information are conducted by the foreign entity; and
- The importance of the foreign entity to a Canadian industry.[145]

4.9.2 Are there specific rules for breaches caused online (when the information is accessible from different jurisdictions)?

No. The rules above would apply equally in relation to online breaches.

4.10 From your experience, what reforms should be made to the legal system of your country to better protect individual privacy, if any?

There are several proposed reforms to *PIPEDA* that are currently before Parliament which aim to better protect the personal information of all Canadians surfing the internet and making online purchases. These reforms are currently before being considered by the House of Commons in Bill S-4, entitled "*An Act to amend the Personal Information Protection and Electronic*

---

[144] *Lawson v. Accusearch Inc*., 2007 FC 125. See also: PIPEDA Case Summary #365 - Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered - <http://www.privcom.gc.ca/cf-dc/2007/365_20070402_e.asp>.

[145] PIPEDA Case Summary #365 - Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered - <http://www.privcom.gc.ca/cf-dc/2007/365_20070402_e.asp>. See also: Office of the Privacy Commissioner of Canada, *Leading By Example: Key Developments in the First Seven Years of PIPEDA* (2008), < https://www.priv.gc.ca/information/pub/lbe_080523_e.pdf>, at 13-15.

Documents Act and to make a consequential amendment to another Act."[146] Bill S-4 is also known the *Digital Privacy Act.* Several noteworthy reforms are noted below:

4.10.1 Breach Notification

Bill S-4 proposes to add three new sections to *PIPEDA* dealing with breaches of security safeguards. These sections have been proposed in the wake of several high profile breaches of large corporations by computer hackers which exposed the personal information of many Canadians. They aim to encourage Canadian corporations to implement sufficient security measures to prevent these types of breaches in the future. An organization that has experienced a breach of security safeguards involving personal information under its control will be required to notify the following parties in three circumstances:

- to the Privacy Commissioner "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual";
- to the individuals whose personal information is involved "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual"; and
- to other organizations or government institutions if the notifying organization believes that the other organization or the government institution may be able to reduce the risk of harm that could result from the data breach or mitigate that harm.

Bill S-4 proposes to define a breach of security safeguards as "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards." The definition of "significant harm" is an open-ended definition that includes: bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.[147]

4.10.2 Offences for Failure to Comply with Breach Notifications

Clause 24 of Bill S-4 proposes to modify section 28 of *PIPEDA*, whereby any organization which knowingly contravenes the new provisions on reporting obligations or obstructs the Commissioner in its audit or investigation of a complaint relating to security breaches will be liable for fines up to $100,000 for indictable offences, and fines up to $10,000 for summary conviction offences. [148]

---

[146] Office of the Privacy Commissioner of Canada: *Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act: Comments on Specific Provisions in S-4*, (June 4, 2014), < https://www.priv.gc.ca/parl/2014/parl_sub_140604_sen_e.asp> ["*Bill S-4*"].
[147] *Ibid.*
[148] Library of Parliament, *Legislative Summary: Bill S-4,* Publication No. 41-2-S4- E, (June 11, 2014), < http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/41/2/s4-e.pdf>, at 11.

4.10.3 Disclosures in Connection with Investigations

Section 7(3)(d) of *PIPEDA* currently provides that an organization can disclose personal information, without the knowledge or consent of the individual, to an investigative body when there are "reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed."[149]

Bill S-4 proposes to eliminate the investigative body regime above with two new paragraphs 7(3)(d.1) and 7(3)(d.2). They will allow an organization to disclose personal information without consent to another organization if:

- it is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation; or

- it is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud.[150]

5 Interplay Between Data Protection Rules and Privacy Rights

5.1 Summarize how data protection law in your jurisdiction protects privacy or other personal data being used in online media.

Canada does not have legislation that is similar in breadth to the European Union's *Data Protection Directive*. Rather, online privacy protections for Canadians stem from application of *PIPEDA* to the online world, and also from our courts.

5.1.1 *PIPEDA* and Online Privacy

PIPEDA or the provincial equivalents apply to the collection, use and disclosure of personal information, whether the personal information is in tangible or digital form. The Commissioner has investigated complaints made under *PIPEDA* against social media companies, including Google, Facebook and WhatsApp.[151]

The Commissioner has also released a policy paper on *PIPEDA*'s application to the controversial practice of online behavioural advertising ("OBA"), which involves tracking a person's online browsing history in order to create and direct advertisements tailored to that user's (sometimes

[149] *Bill S-4*, *supra* note 146.
[150] *Ibid.*
[151] For the final decisions of the OPCC investigations, please visit Findings under the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), The Office of the Privacy Commissioner of Canada, online: <https://www.priv.gc.ca/cf-dc/pi_index_e.asp>.

very specific) interests.[152] Although much of the data at issue would not in isolation constitute "personal information" under section 2 of *PIPEDA*, the Commissioner concluded that the disparate pieces of data in aggregate are capable of identifying the user in many circumstances. As a result, organizations engaging in OBA must be *PIPEDA*-compliant and obtain individual consent: the fact that OBA is occurring must be disclosed and there must be a mechanism in place to opt-out of OBA.

When it comes to online security and mandatory data breach notification, most of Canada lags behind its American and European counterparts.[153] Canadian organizations are currently not obligated to notify the affected individual or the privacy commissioner where its network is hacked, thereby unintentionally disclosing personal information data. Mandatory breach notifications are currently being debated by Parliament in proposed amendments to *PIPEDA*, and are expected to become law, as discussed above.[154]

5.1.2 Charter Jurisprudence

Less than one year ago, the Supreme Court of Canada ruled that online users have a reasonable expectation that their online browsing activity will be anonymous.[155]

To give this ruling context, the accused in *Spencer* applied to have evidence excluded from criminal proceedings against him on the basis that the evidence was obtained in a way that violated his rights under the *Charter*.[156] Section 8 of the *Charter* specifically protects Canadians against unreasonable search and seizure by the state. In determining whether this right has been violated, our Court must consider whether an applicant has a reasonable expectation of privacy in the subject of the search.

The police in *Spencer* identified his IP address as being associated with a collection of child pornography in a shared folder accessible to other online users. The Internet Service Provider ("ISP") voluntarily complied with a warrantless request to disclose contact information associated with that IP address.

The Supreme Court held that the police must first obtain a warrant before making such requests.[157] Although disclosure of contact information *per se* may not strike the core of a *Charter*-protected privacy interest, the Supreme Court iterated that the actual matching of a person's identity with browsing activity is deeply personal in nature.

Although the *Charter* is not engaged between two private parties, the relationship between ISPs and subscribers are regulated by *PIPEDA*. ISPs were commonly complying with requests such as

---

[152] The Office of the Privacy Commissioner of Canada, Policy Position on Online Behavioural Advertising, online: <https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp>.
[153] Alberta is the only province to incorporate data breach response obligations into its personal information protection legislation, though notification is required with respect to private health information in Ontario, New Brunswick and Newfoundland.
[154] *Bill S-4*, *supra* note 146.
[155] *R v Spencer*, 2014 SCC 43 [*Spencer*].
[156] *Supra* note 26.
[157] The evidence at issue in *Spencer*, however, was not ultimately excluded for reasons outside of the scope of this paper.

the one made in *Spencer*, as paragraph 7(3)(c.1) of *PIPEDA* provides that organizations may disclose personal information without the knowledge or consent of the individual affected where the request is made by a government institution that has identified its lawful authority to make such a request. *Spencer* makes it clear that such requests must be accompanied with a warrant before ISPs can rely on this provision of *PIPEDA*.

Further, the Supreme Court rejected the argument that consent to the disclosure of personal information, a cornerstone of *PIPEDA*, is implied where the ISP contract contains a term providing that subscriber information may be shared with law enforcement.

5.2 Is there an effective a right of opposition to collection of data?

As consent to the collection, use and disclosure of personal information is a cornerstone of *PIPEDA*, a lack of consent equates to an effective right of opposition.

The Commissioner has established guidelines to obtaining online consent.[158] Privacy policies must be readily available online, and should contain a full description of what information is collected, for what purposes it is used, and with whom and why it is being shared.

Organizations have many options for obtaining online consent, such as clicking an "I agree" button or ticking off a check box. Consent can sometimes be inferred where an opt-out option has not been exercised. Organizations are free to come up with architecture that works best in a given environment, keeping in mind that consent should be expressed in an appropriate form depending on the nature of the information, the context, and the reasonable expectations of users. Many organizations present this request for consent as a contract of adhesion. Often, an organization will require some personal information in order to deliver the requested product or service. If an individual refuses to provide the required information, service may be refused. However, individuals cannot be forced into providing consent for sharing information that is over and above what the organization requires to fulfil a specific purpose.

6 Right to be Forgotten

6.1 Is there a statutory or case-law based "right to be forgotten" in your jurisdiction (whether under domestic or supranational law)? Describe it briefly.

Our understanding of the right to be forgotten is premised primarily on our understanding of that right as enunciated by the Court of Justice of the European Union in *Google v AEPD* ("*AEPD*").[159] Our understanding of *AEPD* is that individuals have the right to require search engines (and possibly other similar intermediaries) to delist links to their personal information under certain circumstances. These circumstances would include, for example, if such information were inaccurate, inadequate, irrelevant or excessive. Whether or not an organization would be compelled to do so would also be subject to balancing the interests of the individual against other fundamental freedoms, such as the freedom of expression. However, the Court in

[158] Office of the Privacy Commissioner of Canada, *Guidelines for Online Consent*, online: <https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp>.
[159] C-131/12 <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>

AEPD concluded that in this particular cases, the interests of the individual would take precedence over the general public's interest in finding such information.

The court's ruling appears to be founded based on its interpretation of Article 12 of the *1995 Data Protection Directive*.[160] That article sets out that:

> Member States shall guarantee every data subject the right to obtain from the controller:
>
> …
>
> (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
>
> (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

While we are not aware of any case in Canada that has enunciated a right to be forgotten similar to that set out in *AEPD*, it should be noted that principles similar to those set out in Article 12 are found in *PIPEDA*. For example, Principle 9 of Schedule 1 of PIPEDA states, in part, that "[w]hen an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question."

Thus, while there does not currently appear to be a right to be forgotten in Canada, the underlying principles which established such a right in Europe do exist in Canada, leaving open the possibility that such principles could be used to establish a similar right. However, for the reasons discussed in the following section, we believe that to be rather unlikely.

6.2 Is there relevant case law in your jurisdiction regarding the right to be forgotten and/or are there other guidelines (whether under domestic or supranational legal procedure) for a successful claim under the right to be forgotten?

To the extent that search engines may be compelled to remove links to sources containing personal information, as was the case in *AEPD*, Canada may be hesitant to adopt a full-blown right to be forgotten.

In a defamation law context, and after carefully balancing the competing interests of freedom of expression and the protection of one's online reputation, the Supreme Court of Canada recognized a distinction between publishing material online versus merely linking to it.[161]

---

[160] Directive 95/46/EC <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>
[161] *Crookes*, *supra* note 116.

The defendant in *Crookes* (before being sued by the plaintiff) wrote an article about the plaintiff's defamation suits and hyperlinked to the allegedly defamatory material at issue. The defendant refused to comply with the plaintiff's request to remove the hyperlinks, and the plaintiff then sued the defendant on the basis that providing hyperlinks to defamatory material equals the publication of defamatory material.

The Supreme Court held it was necessary to rule that hyperlinking (without more) does not constitute publication for the purposes of defamation law. In so deciding, the majority concluded that the free flow of information on the Internet, and freedom of expression as a result, would be impaired if such restrictions were imposed.

Given that the Supreme Court ruled in favour of freedom of expression even when the link in question served to further publicize information that was found to be defamatory and would therefore clearly cause further harm to an individual, we believe that it would be unlikely that courts in Canada would recognize, under privacy principles, a right to remove links to personal information in situations where such information is merely outdated or irrelevant, particularly in the case of links to personal information published for journalistic purposes, as the linked information would be outside the scope of PIPEDA.[162]

6.3 Did the view on the right to be forgotten change in your jurisdiction due to the European Court of Justice Case in Google Spain v. AEPD and González (C-131/12)? Is there any case law arising from this decision in your jurisdiction?

No. Please see Section 6.2 above.

7. Are there other aspects to take into consideration in your jurisdiction in relation to freedom of speech, the privacy right and the right to be forgotten?

No.

[162] It may be of interest to note that the Court in *AEPD* referenced a similar journalistic exception in the 1995 Data Protection. However, somewhat curiously, it indicated that while that exception could apply to the original publisher of information, it would not apply to a search engine indexing such information.

Appendix A

PIPEDA creates a framework whereby personal information about an identifiable individual can only be used with the consent of that individual. Section 5(1) of *PIPEDA* requires that every organization comply with a set of ten principles set out in Schedule 1 of the Act. The ten principles are as follows:

1. Accountability

The accountability principle requires an organization to designate an individual or individuals who are accountable for the organization's compliance with the PIPEDA principles.[163] The individual need not be named in the policy, however, the identity of the individual responsible must be made known upon request.[164]

2. Identifying Purposes

An organization must identify the purposes for which information is collected at or before the time the information is collected, and must document the purposes for which the information is collected.[165] The organization must collect only that information necessary for the purposes that have been identified.[166]

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose must be identified to the person who provided the information prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that new purpose.[167]

3. Consent

Knowledge and consent is required for the collection, use or disclosure of personal information.[168]

An organization must obtain consent in order to collect, use or disclose personal information.[169] This means organizations must make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.[170] The purpose must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.[171]

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of information beyond that required to

[163] *Supra* note 2, Schedule 1, s 4.1.
[164] *Ibid*, Schedule 1, s 4.1.2.
[165] *Ibid*, Schedule 1, s. 4.2 & 4.2.1.
[166] *Ibid*, Schedule 1, s 4.2.2.
[167] *Ibid*, Schedule 1, s 4.2.4.
[168] *Ibid*, Schedule 1, s 4.3.
[169] *Ibid*, Schedule 1, s 4.3.1.
[170] *Ibid*, Schedule 1, s 4.3.2.
[171] *Ibid*, Schedule 1, s 4.3.2.

fulfil the explicitly specified and legitimate purposes indicated for the collection of the information.[172]

In obtaining consent, the organization should take into consideration the reasonable expectations of the individual giving consent. For example, a person buying a subscription to a magazine should reasonably expect that the organisation would also contact the person to solicit the renewal of the subscription. In such a situation the organization can assume that the individual's request constitutes consent for other specific purposes. However, an organization shall not obtain consent through deception.[173]

The way in which consent is sought may vary. Consent can be either express or implied. Express consent is required where the information collected is likely to be sensitive. Implied consent is appropriate where the information is less sensitive.[174] For example, PIPEDA indicates that the names and addresses of subscribers to a newsmagazine would not be considered sensitive information, and therefore implied consent may be suitable for the use of that information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive, requiring express consent.[175]

Individuals can give express consent in many ways, including:

- An application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information.
- A check-off box
- Consent may be given orally
- Consent may be given at the time that individuals use a product or service[176]

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such a withdrawal.[177]

4. Limiting Collection

The collection of personal information must be limited to that which is necessary for the purposes identified by the organization.[178] Organizations shall not collect personal information indiscriminately. Organizations shall specify the type of information collected as part of their information-handling policies and practices.[179]

[172] *Ibid*, Schedule 1, s 4.3.3.
[173] *Ibid*, Schedule 1, s 4.3.5.
[174] *Ibid*, Schedule 1, s 4.3.6.
[175] *Ibid*, Schedule 1, s 4.3.4.
[176] *Ibid*, Schedule 1, s 4.3.7(a)-(d).
[177] *Ibid*, Schedule 1, s 4.3.8.
[178] *Ibid*, Schedule 1, s 4.4.
[179] *Ibid*, Schedule 1, s 4.4.1.

5. Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.[180]

Organizations using personal information for a new purpose shall document this purpose.[181]

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods.[182]

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous. Organizations must develop guidelines and implement procedures to govern the destruction of personal information.[183]

Care shall be used in the disposal or destruction of personal information to prevent unauthorized parties from gaining access to the information.[184]

6. Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.[185]

7. Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.[186]

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.[187] The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information and the method of storage. More sensitive information should be safeguarded by a higher level of protection.[188]

Methods of protection should include:

- Physical measures, such as locked filing cabinets and restricted access to offices;

[180] *Ibid*, Schedule 1, s 4.5.
[181] *Ibid*, Schedule 1, s 4.5.1.
[182] *Ibid*, Schedule 1, s 4.5.2.
[183] *Ibid*, Schedule 1, s 4.5.3.
[184] *Ibid*, Schedule 1, s 4.7.5.
[185] *Ibid*, Schedule 1, s 4.6.
[186] *Ibid*, Schedule 1, s 4.7.
[187] *Ibid*, Schedule 1, s 4.7.1.
[188] *Ibid*, Schedule 1, s 4.7.2.

- Organizational measures, for example, security clearances and limiting access on a "need-to-know" basis;
- Technological measures, for example, the use of passwords and encryption.[189]

Organizations must make their employees aware of the importance of maintaining the confidentiality of personal information.[190]

8. Openness

An organization must make readily available to individuals specific information about its policies and practices relating to the management of personal information.[191]

Organizations must be open about their policies and practices with respect to the management of personal information. Individuals must be able to acquire information about an organization's policies and practices without unreasonable efforts.[192]

The information made available must include:

a) The name or title and address of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
b) The means of gaining access to personal information held by the organization;
c) A description of the type of personal information held by the organization, including a general account of its use;
d) A copy of any brochures or other information that explain the organization's policies, standards or codes;
e) What personal information is made available to related organizations.[193]

9. Individual Access

Upon request, an individual must be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information.[194] An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.[195]

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual.[196] The organization shall allow the individual access to this information.[197] The organization must provide an account of the use that has been made or is

[189] *Ibid*, Schedule 1, s 4.7.3.
[190] *Ibid*, Schedule 1, s 4.7.4.
[191] *Ibid*, Schedule 1, s 4.8.
[192] *Ibid*, Schedule 1, s 4.8.1.
[193] *Ibid*, Schedule 1, s 4.8.2.
[194] *Ibid*, Schedule 1, s 4.9.
[195] *Ibid.*
[196] *Ibid*, Schedule 1, s 4.9.1.
[197] *Ibid.*

being made of this information and an account of the third parties to which it has been disclosed.[198]

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual.[199] Section 8(3) of PIPEDA requires an organization to respond to such a request within 30 days of receipt of the request for information.[200]

Where a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization.[201]

10. Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.[202]

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information.[203] The compliant procedures should be easily accessible and simple to use.[204]

[198] *Ibid.*
[199] *Ibid*, Schedule 1, s 4.9.4.
[200] *Ibid*, s 8(3).
[201] *Ibid*, Schedule 1, s 4.9.6.
[202] *Ibid*, Schedule 1, s 4.10.
[203] *Ibid*, Schedule 1, s 4.10.2.
[204] *Ibid.*