A Secured Creditor's Ability To Sell Assets Containing Personal Information[1]

By Philip Cho,

Kronis Rotsztain Margles Cappel LLP

When a secured creditor looks to enforce its rights and exercise its remedies, it must be aware of potential privacy issues raised by the application of the *Personal Information Protection and Privacy Act* ("PIPEDA").[2] A secured creditor may be required to deal with the personal information of individuals with whom it does not have any direct relationship with.

Privacy issues as between secured creditor and debtor are generally dealt with through the specific exceptions provided in PIPEDA with respect to investigating a breach of an agreement and for collecting a debt. For example, a secured creditor is often required to give notice to third parties and in so doing, will require the personal information of other persons, some of whom may be individuals. The information required to provide notice would be not much more than name and address information, which is normally obtained from a search of the *Personal Property Security Act* Registry. This would fall under the "publically available" exception in paragraphs 7(1)(d), 7(2)(c.1) and 7(3)(h.1) of PIPEDA which according to the regulations made under PIPEDA include:

> (c) personal information that appears in a registry collected under a statutory authority and to which a right of public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry.[3]

[1] I would like to express my gratitude for the time and effort provided by Adam Nathanson, articling student with the firm, in assisting me with this paper.

[2] *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5, as amended.

[3] Section 1(c), *Regulations Specifying Publicly Available Information*, SOR/2001-7.

However, real issues can arise where the secured creditor seeks to sell accounts, a business as a going concern or, or other interests in a relationship involving a third party individual. The secured creditor will want to disclose to a potential purchaser the information of the debtor's customers (or tenants, or account holders, or debtors, or patients, etc. depending on the business of the debtor) to assess the value of the collateral, and may ultimately want to make use of the personal information.

There is no exception set out in PIPEDA that expressly permits this sort of use and disclosure, unlike in Alberta and British Columbia where "substantially similar" legislation has been enacted.[4] In both the Alberta and B.C. statutes, there is an exception for business transactions which permits an organization to collect, use and disclose personal information without the consent of the individuals if the parties have entered into an agreement limiting the use, collection and disclosure of the personal information and the information is necessary for determining whether to proceed and for the completion of the transaction. In addition, if the transaction is completed, the organization may collect, use and disclose the personal information without consent if the parties have entered into an agreement in which the purchaser undertakes to use and disclose the information in accordance with the original purpose and the information is related to the operation of the business. There are also provisions for the destruction or return of the information if the transaction does not proceed.

However, where the seller in a proposed business transaction is a secured creditor acting under its security agreement, it is not the "organization" contemplated in the wording of the exceptions.

[4] In Alberta, the *Personal Information Protection Act,* S.A. 2003, c. P-6.5, as amended; In British Columbia, the *Personal Information Protection Act,* S.B.C. 2003, c. 63, as amended.

In other words, the secured creditor is not the original "collector" of the personal information. Both Alberta and B.C. statutes are silent as to that situation.

Another scenario that could give rise to real privacy concerns is where the asset being realized is itself personal information. With the advent of dot-com businesses that do not operate as traditional "brick and mortar" businesses and therefore, may not have traditional "assets", personal information has proven to be a valuable commodity.[5] PIPEDA does not permit the sale of personal information by the collecting organization without the consent of the individual. One should also note that the business transaction exceptions, in both Alberta and B.C. do not apply to a transaction where the asset is primarily personal information.

PIPEDA or the Privacy Commissioner's office does not provide any express guidance in this regard. However, a review of the following reveals what appears to be a clear recommendation for the treatment of personal information:

1. Provisions of the *Personal Information Protection and Electronic Documents Act*;
2. The Commissioner's Findings and Reports;
3. The jurisprudence dealing with intangibles and confidential information;
4. The Commercial List Model Order for Receiverships;
5. Bill C-29.

[5] Stoddart, Jennifer, "Privacy in the Era of Social Networking: Legal Obligations of Social Media Sites" (2011), 74 Sask. L. Rev. 263 at ¶7.

1. PIPEDA: KEY CONCEPTS

On January 1 2001, with the stated goal of protecting the privacy of individuals and their personal information, Canada's federal government introduced PIPEDA, which has been in effect to private businesses for more than 7 years now. It applies to every organization in respect of personal information that the organization collects, uses, or discloses in the course of commercial activities.[6]

"Personal Information"

PIPEDA defines personal information as information about an identifiable individual which includes any personal information, recorded or not, in any form, including digital or paper format.[7]

The legislation does not narrow this broad definition of personal information. Jurisprudence indicates that personal information is information which, if disclosed together with some other form of publicly available information, would allow a person to be identified.[8] The result is that the range of information that can be deemed to be "personal information" is virtually unlimited as technology changes. Thus, PIPEDA was broad enough to apply to data being collected and interpreted by the *Google Street View* photography vehicle in the *Google* case.[9]

[6] PIPEDA, s. 5(3).
[7] PIPEDA, s. 2(1).
[8] *Girao v. Grossman,* [2011] F.C.J. No. 1310 at ¶32.
[9] PIPEDA Case Summary # 2011-001, where the vehicle had software for detecting the location of publically broadcast wi-fi locations, however the software contained code which interpreted the data being collected to reveal additional information about the traffic on the wi-fi network including telephone numbers and addresses.

"Consent"

The concept of "consent" is of great importance under PIPEDA. Consent can be express (positive or opt-in), deemed (negative option or opt-out) or implied. For consent to be valid under PIPEDA, it must be meaningful. In fact, PIPEDA actually requires "knowledge and consent" of the individual.[10] The opt-in consent requires some form of affirmative action by the individual, such as the clicking of a box or a signature. In the alternative, an opt-out consent is when an individual is deemed to consent through their non-response to a privacy notice, for example language within an agreement which allows an individual to opt-out of certain uses, disclosures, or collection of their personal information. Generally, opt-out consent is discouraged and is limited in its use to clearly non-sensitive information and the procedure for opting-out must be convenient and easy.[11]

It is this principle that prevents organizations from creating privacy policies that are overly broad and vague in an attempt to effectively get consent *carte-blanche*.

"Collection, Use and Disclosure"

The "knowledge and consent" requirements concern three activities: collection, use and disclosure. Separate knowledge and consent is required for each of the three activities and the consent to one activity does not imply consent for another activity.[12]

Even if an organization does not directly collect the information, an organization has an obligation to ensure (unless an exception applies) that the personal information was collected in

[10] PIPEDA, *supra,* Schedule 1, Principle 3, 4.3.
[11] PIPEDA Case Summary #2003-207.
[12] PIPEDA, *supra*, Schedule 1, Principle 3, 4.3.1.

accordance with PIPEDA, and that it is being disclosed to the organization in accordance with PIPEDA, and that the organization's intended use was consented to in accordance with PIPEDA.[13]

"Reasonable Purpose"

Subsection 5(3) of PIPEDA contains a reasonableness standard and prohibits the collection, use and disclosure of personal information unless for a purpose that a reasonable person would consider is appropriate in the circumstances.[14]

The corollary to this is that the collection, use and disclosure conducted by an organization can be deemed to be reasonable (and therefore permissible) despite the express objections of an individual (unreasonable) complainant.[15]

Exceptions in PIPEDA

There are a number of exceptions to the collection, use and disclosure requirements. The exceptions that could be used in the realization of security are as follows:

[13] See for example PIPEDA Case Summary #2009-017 where in a complaint involving landlords, tenants and a third party organization which provided background checks for landlords, the service agreement between the organization and the landlords contained language requiring the landlords to have the consent of the tenants before requesting information. Based on this, the Assistant Commissioner determined that it was reasonable that the organization presumed consent for certain purposes but not all.

[14] PIPEDA, *supra*, s. 5(3).

[15] See for example, PIPEDA Case Summary #2009-011 where a transit driver objected to the use of GPS and similar technology to track the organization's vehicles. Despite the driver's objections, the Privacy Commissioner found that it was reasonable for the organization to assume it had implied consent and the use of the personal information collected was appropriate under section 5(3).

I. Collection[16]: 7(1):

(a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;

…

(d) the information is publicly available and is specified by the regulations;

(e) the collection is made for the purpose of making a disclosure… (ii) that is required by law.

II. Use[17]: 7(2):

…

(c.1) it is publicly available and is specified by the regulations;

(d) it was collected under paragraph (1)(*a*), (*b*) or (*e*).

III. Disclosure[18]: 7(3):

(a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;

(b) for the purpose of collecting a debt owed by the individual to the organization;

(c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

…

(h.1) of information that is publicly available and is specified by the regulations;

(h.2) made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;

(i) required by law.

[16] PIPEDA, *supra*, s. 7(1).
[17] PIPEDA, *supra*, s. 7(2).
[18] PIPEDA, *supra,* s. 7(3).

2. THE PRIVACY COMMISSIONER

PIPEDA created the Office of the Privacy Commissioner, a position which responds to or initiates complaints against organizations which contravene the Act. The Privacy Commissioner reports directly to the House of Commons and the Senate, and publishes her findings for public dissemination on a government website.[19] The Privacy Commissioner has the power to investigate complaints, including the ability to summon witnesses, compel testimony, produce and examine records, administer oaths, and enter any premises occupied by an organization other than a dwelling house.[20] After investigating any complaint, the Commissioner issues a report indicating their findings, recommendations, any settlement reached by the parties, and notice of any actions taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been taken.[21]

Should the complainant remain unsatisfied with the Commissioner's finding, the complainant may, after receiving the Commissioner's report or being notified that the investigation of the complaint has been discontinued, apply to the Court for a hearing on the matter.[22] This hearing is a *de novo* review of the Commissioner's findings and recommendations.[23] Upon hearing the complaint, the Court may make an order for the organization to correct its practices, order that the organization publish a notice of any action taken or proposed to be taken to correct its practices, or award damages to the complainant.[24] At the hearing, it is the conduct of the party

[19] Office of the Privacy Commissioner of Canada (online: http://www.priv.gc.ca/index_e.cfm).
[20] PIPEDA, *supra,* s. 12.1.
[21] PIPEDA, *supra,*s. 13(1).
[22] PIPEDA, *supra,*s. 14(1).
[23] *Randall v Nubodys Fitness Centres*, 2010 FC 681 at ¶32.
[24] PIPEDA, *supra* s. 14(3).

against whom the complaint was filed which is at issue, not the Commissioner's report.[25] The jurisprudence enumerates certain non-exhaustive factors which could be applied to PIPEDA applications for damages, such as whether awarding damages would further the general objects of PIPEDA and uphold the values which it embodies, whether damages awarded would deter future breaches, and the seriousness or egregiousness of the breach.[26]

Case Summaries

Surprisingly, a search of the Privacy Commissioner's findings for the term "secured creditor" returns no hits. However, the following are some other cases that provide some guidance.

PIPEDA Case Summary #2006-350: This case involved two different complaints from individuals who were not warned of the transfer of their credit card accounts, and therefore their personal information, from one bank to another.

In the first complaint, the Commissioner found that the bank did not violate PIPEDA as they mailed all of their cardholders a revised agreement with an assignment clause approximately 2 years before the sale of their credit card accounts. This assignment clause provided notice to the cardholder that the bank could transfer by way of assignment, sale or otherwise, a customer's account. Through this transfer, the bank reserved the right to give information about the cardholder's account to anyone, so long as the transferee maintained the cardholder's privacy rights.

[25] *Englander v Telus Communications Inc.*, 2004 FCA 387 at ¶47-48.
[26] *Mirza Nammo v. Transunion of Canada Inc.,* 2010 FC 1284 at ¶76.

In the second complaint, the bank was found *not* to be in compliance with PIPEDA. Although the *Bank Act* permitted the sale of assets by a bank (including the credit card accounts), the credit card agreement in this case did not have a similar assignment clause as in the first complaint. The complaint was determined to be well-founded.

These two complaints illustrate the relatively simple manner in which one can obtain consent in advance by incorporating appropriate terms in a service agreement or privacy policy. If such precautions are not taken, then despite other legal rights permitting the transfer of assets, the disclosure of personal information will still be grounds for an adverse finding under PIPEDA.

PIPEDA Case Summary #2006-325: After reading a consent form, a patient of a dentist complained about the potential sale of his personal information in the sale of the dental practice. The Commissioner found no violation of PIPEDA as a reasonable person would consider it appropriate that a dentist disclosed patient personal information to prospective buyers in order to evaluate the worth of the practice so long as the transferor and transferee maintained the original confidentiality agreements.

This complaint occurred before the enactment of the Personal Health Information Protection Act *which expressly permits this type of disclosure. Thus, it is illustrative of how the Privacy Commissioner interprets the "reasonable purpose" principle in PIPEDA. It appears from the summary that the consent form provided by the dental office contained language that contemplated a potential sale of the practice.*

PIPEDA Case Summary #2008-394: This case involved the outsourcing of personal information to a third party service provider. The Assistant Commissioner determined that if the purpose of the current provider's use of the personal information remained the same, organizations were not required to obtain renewed customer consent for the information's use, so long as the organization obtained valid consent for the provision of services or products at the outset.

One of the findings made by the Assistant Commissioner was that the "service agreement between the two parties relies on unambiguous language that provides guarantees of the confidentiality and security of personal information, and it allows for oversight, monitoring and audit of the services being provided." This case illustrates the relevance of contractual terms between the original holder of the information and the third party that restrict and determine the extent to which the personal information can be used by the third party.

PIPEDA Case Summary #2009-017: This case an organization that was collecting and using sensitive personal information about tenants and disclosing the information to the organization's paying members (i.e., landlords). Although the organization was not directly collecting the information from tenants, it received the information and would use and disclose such information.

The organization had a minimum obligation to demonstrate due diligence with respect to consent and must have in place appropriate contractual terms stipulating that the members are collecting the information with appropriate consent.

3. Intangibles and Duty of Confidentiality

A. Intangibles

The current Privacy Commissioner of Canada, Jennifer Stoddart, wrote that social networking has "helped transform personal information into a commodity, which is increasingly being "scraped" from online fora and sold to companies that use it to target advertising, among other things."[27] The value of being able to collect and use personal information is undeniable. With the restrictions placed on the collection, use and disclosure of personal information, will personal information be realizable as collateral?

The PPSA defines "intangibles" as "all ***personal property***, including choses in action, that is not goods, chattel paper, documents of title, instruments, money or investment property."[28] In a somewhat circular fashion, "personal property" is defined as "chattel paper, documents of title, goods, instruments, ***intangibles***, money and investment property, and includes fixtures but does not include building materials that have been affixed to real property."[29]

In *Saulnier v. Royal Bank of Canada*, a case involving fishing licences, the Supreme Court grappled with the meaning of "intangibles" when the collateral secured by a general security agreement over a fishing business would only have real value if the fishing licences could be sold with the business. In making its decision in favour of the creditor's expectations, the Supreme Court defined the court's role as being "[to] interpret the definitions in the *BIA* and the

[27] Stoddart, Jennifer, "Privacy in the Era of Social Networking: Legal Obligations of Social Media Sites" (2011), 74 Sask. L. Rev. 263 at ¶7
[28] PPSA, *supra*, s. 2 [emphasis added].
[29] PPSA, *supra,* s. 2 [emphasis added].

PPSA in a purposeful way having regard to "their entire context, in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.""[30]

The Court described the nature of the fishing licence as follows:

> As described above, the holder of a s. 7(1) licence acquires a good deal more than merely permission to do that which would otherwise be unlawful. The holder acquires the right to engage in an exclusive fishery under the conditions imposed by the licence and, what is of prime importance, a proprietary right in the wild fish harvested thereunder, and the earnings from their sale. While these elements do not wholly correspond to the full range of rights necessary to characterize something as "property" at common law, the question is whether (even leaving aside the debate about the prospects of renewal) they are sufficient to qualify the "bundle of rights" the appellant Saulnier did possess as property for purposes of the statutes.[31]

The Court found that the definition of property in the *BIA* clearly signaled an intention by Parliament to "sweep" up a variety of assets of the bankrupt not normally considered "property" at common law,[32] while the purpose of the *BIA* was "to regulate the orderly administration of the bankrupt's affairs, keeping a balance between the rights of creditors and the desirability of giving the bankrupt a clean break."[33] The Court also noted that the *PPSA* was a statute that is designed to facilitate the creation of a security interest to enable holders of personal property to use it as collateral, and to enable lenders to predict accurate the priority of their claims against the assets in question.[34]

---

[30] *Saulnier v. Royal Bank of Canada,* 2008 SCC 58 at ¶16 quoting R. Sullivan, *Sullivan and Driedger on the Construction of Statutes* (4th ed. 2002), at 1. The definition of "property" in the section 2 of the *BIA* includes "obligations, easements and every description of estate, interest and profit… arising out of or incident to property." Section 2 of the *PPSA* defines "personal property" as including an "intangible", which in turn is defined as "personal property that is not goods, a document of title, chattel paper, a security, an instrument or money."
[31] *Saulnier, supra* at ¶43.
[32] *Saulnier, supra* at ¶44.
[33] *Saulnier, supra* at ¶17 citing *Husky Oil Operations Ltd. v. Minister of National Revenue,* [1995] 3 S.C.R. 453 at ¶7.
[34] *Saulnier, supra* at ¶19.

The Supreme Court in *Saulnier* has made it clear that the definition of "property" for the purpose of secured lending and creditor/debtor rights should be flexible enough to accommodate the growing value being ascribed to personal information such as product preferences, purchase histories, click-stream data, Facebook "Likes", Tweets, etc. It is uncontroversial that personal information certainly has a commercial value and therefore, should be treated the way fishing licences were in *Saulnier*.

B. Duty of Confidentiality

Prior to the era of social networking, the tension between the PPSA and the personal information of individuals arose in the context of patient records. *Axelrod (Re)*[35] dealt with the enforcement of a GSA over the property of a dentist, and in particular, the dentist's patient lists and patient files. The secured creditor was finance company in the business of financing the practices of health professionals. It took a security interest by way of a GSA in all of the personal property of the debtor, including patient lists and patient files, of the practice.

The motions judge considered a number of cases regarding the ownership of patient records and in particular, a Supreme Court of Canada decision which stated:

> The patient is not entitled to the records themselves. The physical medical records of the patient belong to the physician. … Information about oneself revealed to a doctor acting in a professional capacity remains, in a fundamental sense, one's own. While the doctor is the owner of the actual record, the information is held in a fashion somewhat akin to a trust and is to be used by the physician for the benefit of the patient.[36]

The motions judge found that the patient records and patient files could be charged and so long as the creditor preserves the patient's rights to confidentiality and to access, the creditor was

[35] *Axelrod (Re)*, 1994 CanLII 3466 (ON CA) aff'g (1994), 16 O.R. (3d) 649 (Gen. Div.).
[36] *Axelrod, supra* (Gen. Div.) at ¶20 citing *McInerney v. MacDonald*, 1992 CanLII 57 (SCC).

entitled to realize and enforce its security against the patient records and patient files by appointing a qualified dentist to assist in the realization of the security and to act as "custodian" of the files. The secured creditor would not itself take possession of the records. The appointed dentist-custodian would write to the patients to notify them of the change and provide the opportunity to transfer the dental records to another practitioner.

The motions judge's decision was upheld on appeal by the Ontario Court of Appeal. In their decision, the Court of Appeal noted that section 17 of the regulations made under the *Dentistry Act* prohibited a dentist from giving information about a patient to a person other than the patient or an authorized representative without consent. The dentist had a common law duty, as well as a statutory duty, to maintain the patient's confidentiality. This duty created an apparent conflict with the dentist's commercial obligation incurred by the granting of a security interest to the creditor.

The Court of Appeal endorsed the motions judge's reasoning in the following passage where the motions judge expressly chose not to follow a prior decision that held that patient information and files could not be charged[37]:

> With great respect, I have some difficulty with the concept that the relationship of trust which undoubtedly exists between doctor or dentist and patient results in the patients' files or records being analogous to trust property for purposes of the B.I.A., that is to say, property in which the bankrupt holds a bare legal title but has no beneficial interest. It seems to me that the case law already establishes that the files or records are property beneficially owned by the medical practitioner. The full use and enjoyment of that property by the medical practitioner is, however, subject to common law and statutory rights of the patient with respect to maintaining confidentiality and with respect to access.

[37] *Axelrod, supra* (C.A.) at ¶ 9 (CanLII). The motions judge was referring to the case of *Josephine V. Wilson Family Trust v. Swartz*, (1993), 16 O.R. (3d) 268 (Gen. Div.) where Blair J. held that while the dental records may be the physical property of the dentist, they are property affixed with an inseverable trust of confidentiality in favour of the patient and could not be property belonging to the dentist for purposes of pledging.

> Property interests subject to certain restrictions or rights of third parties are capable of being charged. In my view, so long as such rights are preserved by the creditor realizing upon its security, that creditor ought not to be deprived of realization and enforcement rights granted pursuant to a security agreement.[38]

The Court of Appeal recognized that the apparent conflict could be avoided if the dentist fulfilled his contractual obligations to the creditor by writing to his patients to inform them that he will turn over their files to a new dentist (to be arranged by the secured creditor) who is taking over his practice, unless he receives other instructions from them. However, the dentist's unwillingness to assist the creditor "should not defeat the right of a *bona fide* creditor to execute on its security, if this can be done with maximum protection for the confidentiality of the information contained in the patients' files."[39]

An issue that was raised but did not get determined by the Court of Appeal related to the breach of confidence that would necessarily occur if the dentist refused to cooperate. If the duty of confidentiality extends to keeping the very existence of the dentist-patient relationship confidential, then that confidence could not be protected without the dentist's cooperation because the creditor would at a minimum require the identity of the patients for the purposes of contact. The Court of Appeal simply noted:

> This is something that the dentist may have to answer for to the appropriate authorities. Meanwhile, the best accommodation of the rights of the creditor and rights of the patients is reflected in Ground J.'s order [the motions judge].[40]

[38] *Axelrod, supra* (Gen. Div.) at ¶24.
[39] *Axelrod, supra* (C.A.) at ¶ 11 (CanLII).
[40] *Axelrod, supra* (C.A.) at ¶ 12 (CanLII).

Axelrod was referred to in a more recent decision of the Alberta Court of Queen's Bench dealing with a sale under the *Companies' Creditors Arrangement Act* ("CCAA") which, in a certain way, brings together the issue in *Saulnier* and the issue in *Axelrod*.

At issue was the status of certain seismic data ("Data") compiled by one of the creditors, Pulse Data Inc. ("Pulse"), but prepared for the debtor, Gauntlet Energy Corporation ("Guantlet"), under conditional sales agreements. Gauntlet granted to Alberta Treasury Branches ("ATB") a general security interest over all of its present and after-acquired property, such that if the Data constituted "personal property" under the PPSA, then Gauntlet's interest rank would ahead of Pulse's interest.[41]

The court held that the Data, while retaining its confidential nature, was property capable of being pledged under the PPSA.[42] The court maintained the long-standing principle that property that is subject to the rights or interest of a third party may still be pledged as security.

4. The Model Receivership Order

The model receivership order used on the Commercial List specifically contemplates this commercial reality. The Explanatory Notes for the Standard Form Template Receivership Order comment on the problem created by PIPEDA as follows:

> The Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 ("PIPEDA") by its terms seems to impact on the ability of creditors to realize upon a business. Personal information concerning employees, customers and possibly suppliers could well be very important components of either a receiver's ability to run the business

[41] *Re Gauntlet Energy Corporation*, 2003 ABQB 718. Although Pulse's interest could have enjoyed super-priority by virtue of purchase-money security interest provisions in the Alberta PPSA, Pulse had failed to register its security interest and could not avail itself of this super-priority.
[42] *Re Gauntlet*, *supra* at ¶38 and ¶46.

> or to sell it. The statute contains a reasonableness standard that is one of the over-riding principles guiding the use and dissemination of personal information. A Receiver has little time nor ability to seek the consent of every employee or every customer before disclosing information needed to keep a plant open or to allow an expeditious realization. The reasonableness of limiting the need to obtain express consent in urgent circumstances in order to keep a business from failing is self-evident. It maintains the jobs and the business to which individuals have provided their information presumably because they either want their jobs or they want to do business with the debtor. PIPEDA also allows for court orders limiting the need to obtain express consent in appropriate circumstances. The standard form template order contains such a limitation drawn from the PSINet Limited CCAA proceeding. In effect, the Receiver will be entitled to disclose personal information to prospective purchasers under the terms of appropriate confidentiality orders and provided that the purchaser, by agreement and court order, can make no further use of the debtor's data than was available to the debtor itself.

The model receivership order language is reproduced below:

> THIS COURT ORDERS that, pursuant to clause 7(3)(c) of the Canada *Personal Information Protection and Electronic Documents Act*, the Receiver shall disclose personal information of identifiable individuals to prospective purchasers or bidders for the Property and to their advisors, but only to the extent desirable or required to negotiate and attempt to complete one or more sales of the Property (each, a "Sale"). Each prospective purchaser or bidder to whom such personal information is disclosed shall maintain and protect the privacy of such information and limit the use of such information to its evaluation of the Sale, and if it does not complete a Sale, shall return all such information to the Receiver, or in the alternative destroy all such information. The purchaser of any Property shall be entitled to continue to use the personal information provided to it, and related to the Property purchased, in a manner which is in all material respects identical to the prior use of such information by the Debtor, and shall return all other personal information to the Receiver, or ensure that all other personal information is destroyed.[43]

5. Bill C-29

Section 29 of PIPEDA requires Parliament to review Part I of the Act every five years.[44] In 2007, after hearing 67 witnesses and submissions from 34 different individuals and organizations, the House Standing Committee on Access to Information, Privacy and Ethics

[43] Form Template Receivership Order ("Model Order") by the Superior Court of Justice - Commercial List.
[44] PIPEDA, *supra,* s. 29(1)

completed this review.[45] Their report concluded that PIPEDA did not require major changes at that moment; however, they made a number of recommendations, including a security breach disclosure provision and new business exceptions.

These recommendations would surface three years later as Bill C-29 "An Act to amend the Personal Information Protection and Electronic Documents Act."[46] Bill C-29 had its first reading in Parliament on May 25, 2010, and a second reading on October 26th, 2010. The new business exceptions were made in response to calls from the business world to help clarify their responsibilities under PIPEDA.[47] Bill C-29 did not make it past the second reading stage and will have to reappear in the next session of Parliament.[48] However, Bill C-29 signals an acknowledgment that PIPEDA requires some adjustment to "facilitate commercial transactionsand protect commercial secrets in a highly competitive environment."[49]

If enacted, Bill C-29 would alter PIPEDA to create a new exception for business transactions based on the Alberta *Personal Information Protection Act* but with enhancements recommended by the Privacy Commissioner. Like the Alberta and BC Acts, and the Model Order, Bill C-29 would allow parties to a prospective business transaction to use and disclose personal information without the knowledge and consent of the individual.

---

[45] House of Commons Debates, 40th Parl, 3rd Sess, No 87 (26 October 2010) at 1615 (Tony Clement).
[46] *Safeguarding Canadians' Personal Information Act*, Bill C-29, 40th Parl., 3rd Sess., 2000, c. 5
[47] House of Commons Debates, supra
[48] Once a Bill makes it past the second reading stage, it moves to a committee for further study, after which, the Bill is brought back before the House of Commons for a third reading and the potential passage of the Bill. Since Bill C-29 was not moved past a second reading before the 40th session of Parliament ended, it will have to reappear in the new session of Parliament.
[49] Office of the Privacy Commissioner of Canada, *Statutory Review of the* Personal Information Protection and Electronic Documents Act: *Background Information on the OPCs Consultation,* November 27, 2006, http://www.priv.gc.ca/parl/2006/sub_061127_e.cfm#009

A "business transaction" would include

- the purchase, sale or other acquisition or disposition of an organization or a portion of an organization, or any of its assets;
- the merger or amalgamation of two or more organizations;
- the making of a loan or provision of other financing to an organization or a portion of an organization;
- the creating of a charge on, or the taking of a security interest in or a security on, any assets or securities of an organization;
- the lease or licensing of any of an organization's assets; and
- the arrangement between two or more organizations to conduct a business activity other than the processing of personal information in the hands of a third party.[50]

Similar to the Alberta and BC models, the Model Order, and the discussions in *Axelrod*, the parties are required to have an appropriate agreement between them that outline the manner in which the third party is permitted to use the personal information. This agreement should state that the use and disclosure of personal information is solely for the purposes related to the transaction, protected by the appropriate security safeguards, and will be returned to its original source within a reasonable time should the transaction not proceed.[51]

There would also be a requirement that the personal information is necessary to determine whether to proceed with the transaction and/or complete the transaction.[52]

[50] Bill C-29, *supra,* s. 2(3)
[51] *Ibid*, s. 7
[52] *Ibid*, s. 7

Again, following the Alberta and BC Acts, the Model Order, and some of the principles discussed in *Axelrod* and *Re Gauntlet,* after the transaction is completed, the third party may use and disclose the personal information without the knowledge or consent of the individual only if the organization agrees to use and disclose the personal information under its control solely for the purposes for which the personal information was collected or permitted to be used or disclosed before the transaction was completed. Bill C-29 however adds that the agreement should provide for the protection of that information by security safeguards appropriate to the sensitivity of the information, and to give effect to any withdrawal of consent made in accordance with PIPEDA's clause 4.3.8 of Schedule 1.

Further, in line with some of the Commissioner's findings, Bill C-29 requires that one of the parties to the transaction notify the individual that their personal information has been disclosed within a reasonable time after the transaction's completion.[53]

Similar to the Alberta and BC models, there remains an important exception to the proposed prospective business transactions exceptions in PIPEDA. The business transaction exception does not apply to a business transaction in which the primary purpose or result of the transaction is the purchase, sale or other acquisition or disposition, or lease, of personal information.[54] Therefore, should the object of the transaction be personal information itself, PIPEDA's new exceptions would not apply.

[53] *Ibid*, s.7
[54] *Ibid,* s. 7

6. Appropriate Purpose

There is a common theme that runs through the Privacy Commissioner's findings, the court's decisions, the Model Order and Bill C-29:

> *As long as the individual's expectations regarding the use of his/her personal information remain respected and preserved, disclosure of personal information in the context of a transfer of assets may be an appropriate disclosure in the circumstances.*

The overarching "reasonable person" standard in s. 5(3) supports this theme as a reasonable person would understand the commercial reality that businesses do get bought and sold at times.

Looking at the case summaries of the Privacy Commissioner that were referred to above, it was important to the Commissioner's findings that:

- the purchaser of the credit card accounts maintained the privacy rights of the individuals;
- any successor dentist maintain the original confidentiality agreements;
- the third party service provider agree to the same use of the personal information as the organization.

In the *Axelrod* and *Gauntlet* cases, the court emphasized that the debtor could only charge the information to the extent of the debtor's interest (i.e. subject to confidentiality rights), and as such, the secured creditor and anyone acquiring through the secured creditor would take subject to such confidentiality rights. In other words, the secured creditor and/or any subsequent acquirer could only deal with the information in the same manner as was required by the debtor.

Bill C-29 makes this express by requiring that organizations that complete a business transaction enter into an agreement that requires each of them:

> to use and disclose the personal information under its control solely for the purposes for which the personal information was collected or permitted to be used or disclosed before the transaction was completed[55]

The review of the Privacy Commissioner's findings and Bill C-29 indicate a strong desire to preserve the individual's privacy expectations. The court's approach has also indicated this desire but permits the exercise of a secured creditor's remedies so long as the confidentiality of the individual is preserved.

In the absence of express authority in PIPEDA or from the court, it is preferable for the secured creditor to have the court's blessing – whether by the appointment of a receiver or by a court order containing a similar provision as in the Model Receivership Order.

However, that may not always be viable for a creditor. In that case, the following is recommended:

1. Review the security agreement regarding the scope of the security and whether it extends to the personal information or whether it provides certain rights to the secured creditor;
2. Determine the nature and extent of personal information collected by the debtor – if it is non-sensitive information then the secured creditor's use may be seen as appropriate for the purpose of the "reasonable person" standard; However, if the information is sensitive, then the appointment of a "custodian" such as in the *Axelrod* case may be appropriate;
3. Review in detail the scope of the consent, whether it is in a privacy policy or in a separate consent agreement – there may be language that refers to a change in ownership or transfer of the business

[55] Bill C-29, *supra* s. 7

4. Determine if it is possible to obtain limited consent from the individuals – this may not be practical from perspectives of timing, cost, maintaining value of security, etc.;
5. Provide for clear contractual terms incorporating the provisions in Bill C-29 regarding limiting purpose, appropriate safeguards to protect the information, return of the information, and subsequent use of the information;
6. As soon as is reasonably practical after the enforcement process, advise the individuals of the transaction as contemplated by Bill C-29.

By adhering as much as is practicable to Bill C-29 and the approach discussed in *Axelrod*, it is reasonable to believe that any necessary collection, use and disclosure by the secured creditor will be considered "appropriate" in the circumstances.